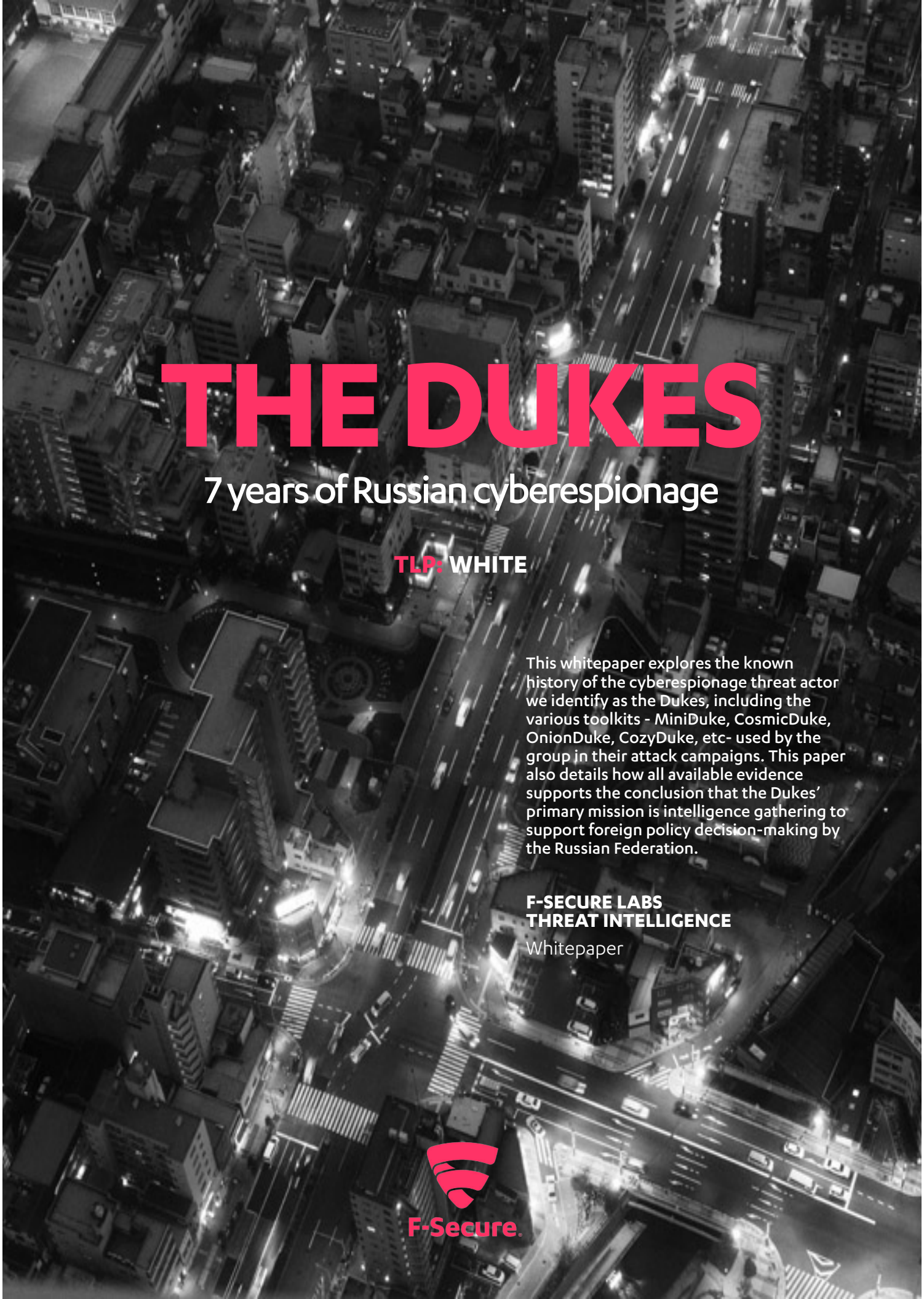


THE DUKES

7 years of Russian cyberespionage

TLP: WHITE

This whitepaper explores the known history of the cyberespionage threat actor we identify as the Dukes, including the various toolkits - MiniDuke, CosmicDuke, OnionDuke, CozyDuke, etc- used by the group in their attack campaigns. This paper also details how all available evidence supports the conclusion that the Dukes' primary mission is intelligence gathering to support foreign policy decision-making by the Russian Federation.

F-SECURE LABS
THREAT INTELLIGENCE

Whitepaper

F-Secure

CONTENTS

EXECUTIVE SUMMARY

The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe have been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States; Asian, African, and Middle Eastern governments; organizations associated with Chechen terrorism; and Russian speakers engaged in the illicit trade of controlled substances and drugs.

The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large-scale spear-phishing campaigns against hundreds or thousands of recipients associated with governmental institutions and affiliated organizations.

These campaigns utilize a smash-and-grab approach, involving a fast but noisy break-in followed by the rapid collection and exfiltration of as much data as possible. If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long-term intelligence gathering.

> ...the Dukes show unusual confidence in their ability to continue successfully compromising their targets [...], as well as in their ability to operate with impunity.

In addition to these large-scale campaigns, the Dukes continuously and concurrently engage in smaller, much more targeted campaigns, utilizing different toolsets. These targeted campaigns have been going on for at least 7 years. The targets and timing of these campaigns appear to align with the known foreign and security policy interests of the Russian Federation of those times.

The Dukes rapidly react to research being published about their toolsets and operations. However, the group (or their sponsors) value their operations so highly that though they will attempt to modify their tools to evade detection and regain stealth, they will not cease operations to do so, but will instead incrementally modify their tools while continuing apparently as previously planned.

In some of the most extreme cases, the Dukes have been known to engage in campaigns with unaltered versions of tools that only days earlier have been brought to the public's attention by security companies and actively mentioned in the media. In doing so, the Dukes show unusual confidence in their ability to continue successfully compromising their targets even when their tools have been publicly exposed, as well as in their ability to operate with impunity.

THE STORY OF THE DUKES

The story of the Dukes, as it is currently known, begins with a malware toolset that we call PinchDuke. This toolset consists of multiple loaders and an information-stealer trojan. Importantly, PinchDuke trojan samples always contain a notable text string, which we believe is used as a campaign identifier by the Dukes group to distinguish between multiple attack campaigns that are run in parellel. These campaign identifiers, which frequently specify both the date and target of the campaign, provide us with a tantalizing view into the early days of the Dukes.

2008: Chechnya

The earliest activity we have been able to definitively attribute to the Dukes are two **PinchDuke** campaigns from November 2008. These campaigns use **PinchDuke** samples that were, according to their compilation timestamps, created on the 5th and 12th of November 2008. The campaign identifiers found in these two samples are respectively, "alkavkaz.com20081105" and "cihaderi.net20081112".

The first campaign identifier, found in the sample compiled on the 5th, references *alkavkaz.com*, a domain associated with a Turkish website proclaiming to be the "Chechan [sic] Informational Center" (image 1, page 5). The second campaign identifier, from the sample compiled on the 12th, references *cihaderi.net*, another Turkish website that claims to provide "news from the jihad world" and which dedicates a section of its site to Chechnya.

Due to a lack of other **PinchDuke** samples from 2008 or earlier, we are unable to estimate when the Duke operation originally began. Based on our technical analysis of the **PinchDuke** we do have, we believe the development of **PinchDuke**, and therefore the Duke operation itself, began no later than the summer of 2008.

In fact, we believe that by the autumn of 2008, the Dukes were already developing not one but at least two distinct malware toolsets. This assertion is based on the oldest currently known sample of another Duke-related toolset, **GeminiDuke**, which was compiled on the 26th of January 2009. This sample, like the early **PinchDuke** samples, appears to already be a "fully-grown" sample, which is why we believe the development of the **GeminiDuke** toolset started no later than the autumn of 2008.

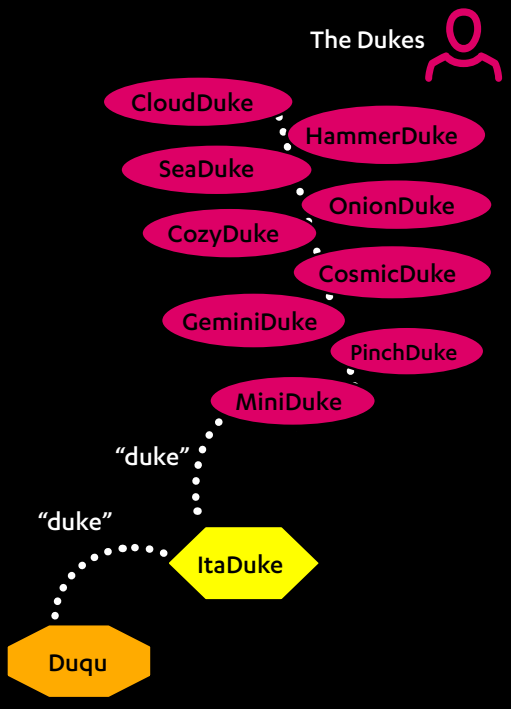
That the Dukes were already developing and operating at least two distinct malware toolsets by the second half of 2008 suggests to us that either the size of their cyberespionage operation was already large enough to warrant such an arsenal of tools, or that they expected their operation to grow significantly enough in the foreseeable future to warrant the development of such an arsenal. We examine each of the Duke toolsets in greater detail later in the Tools and Techniques section (page 16).

Etymology: a note on names

The origins of the Duke toolsets' names began when researchers at Kaspersky Labs coined the term "MiniDuke" to identify the first Duke-related malware they found. As explained in their whitepaper[8], the researchers observed the surprisingly small MiniDuke backdoor being spread via the same exploit that was being used by a malware that they had already named ItaDuke; the "Duke" part of this malware's name had in turn come about because it reminded the researchers of the notable Duqu threat. Despite the shared history of the name itself however, it is important to note that there is no reason to believe that the Duke toolsets themselves are in any way related to the ItaDuke malware, or to Duqu for that matter.

As researchers continued discovering new toolsets that were created and used by the same group that had been operating MiniDuke, the new toolsets were also given "Duke"-derived names, and thus the threat actor operating the toolsets started to be commonly referred to as "the Dukes". The only other publicly used name for the threat actor that we are aware of is "APT29"[23].

Some exceptions to this naming convention do exist, and in the case of specific Duke toolsets, other commonly used names are listed in the Tools and Techniques section (page 16).



2009: First known campaigns against the West

Based on the campaign identifiers found in **PinchDuke** samples discovered in 2009, the targets of the Dukes group during that year included organizations such as the Ministry of Defense of Georgia and the ministries of foreign affairs of Turkey and Uganda. Campaign identifiers from 2009 also reveal that by that time, the Dukes were already actively interested in political matters related to the United States (US) and the North Atlantic Treaty Organization (NATO), as they ran campaigns targeting (among other organizations) a US-based foreign policy think tank, another set of campaigns related to a NATO exercise held in Europe, and a third set apparently targeting what was then known as the Georgian "Information Centre on NATO".

Of these campaigns, two groups in particular stand out. The first is a set of campaigns from the 16th and 17th of April that targeted a US-based foreign policy think tank, as well as government institutions in Poland and the Czech Republic (image 1, below). These campaigns utilized specially-crafted malicious Microsoft Word documents and PDF files, which were sent as e-mail attachments to various personnel in an attempt to infiltrate the targeted organizations.

The second group of note comprises of two campaigns that were possibly aimed at gathering information on Georgia-NATO relations. The first of these runs used the campaign identifier "natoinfo_ge", an apparent reference to the *www.natoinfo.ge* website belonging to a Georgian political body that has since been renamed "Information Centre on NATO and EU". Although the campaign identifier itself doesn't contain a date, we believe the campaign to have originated around the 7th of June 2009, which was when the **PinchDuke** sample in question was compiled. This belief is based on the observation that in all of the other **PinchDuke** samples we have analyzed, the date of the campaign identifier has been within a day of the compilation date. The second campaign identifier, which we suspect may be related, is "mod_ge_2009_07_03" from a month later and apparently targeting the Ministry of Defense of Georgia.

We believe these campaigns had a joint goal of gathering intelligence on the sentiments of the targeted countries with respect to the plans being discussed at the time for the US to locate their "European Interceptor Site" missile defense base in Poland, with a related radar station that was intended to be located in the Czech Republic. Regarding the timing of these campaigns, it is curious to note that they began only 11 days after President Barack Obama gave a speech on the 5th of April declaring his intention to proceed with the deployment of these missile defenses [1] [2].

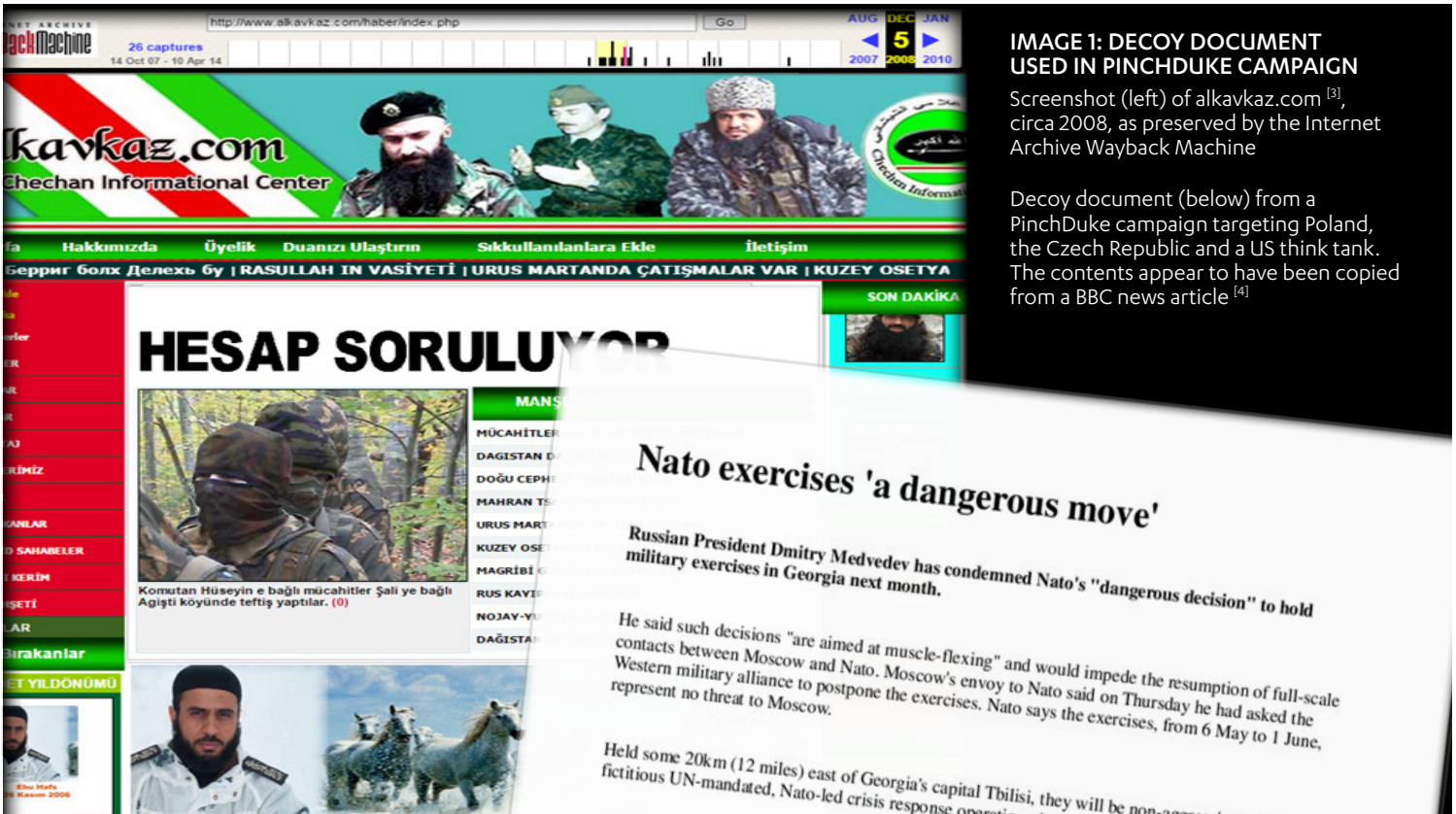


IMAGE 1: DECOY DOCUMENT USED IN PINCHDUKE CAMPAIGN

Screenshot (left) of alkavkaz.com [3], circa 2008, as preserved by the Internet Archive Wayback Machine

Decoy document (below) from a PinchDuke campaign targeting Poland, the Czech Republic and a US think tank. The contents appear to have been copied from a BBC news article [4]

2010: The emergence of CosmicDuke in the Caucasus

The spring of 2010 saw continued **PinchDuke** campaigns against Turkey and Georgia, but also numerous campaigns against other Caucasian states such as Kazakhstan, Kyrgyzstan, Azerbaijan and Uzbekistan. Of these, the presumed Kazakhstan campaign (with the identifier "kaz_2010_07_30") is of note because it is the last **PinchDuke** campaign we observed. We believe that during the first half of 2010, the Dukes slowly migrated from **PinchDuke** and started using a new infostealer malware toolset that we call **CosmicDuke**.

The first known sample of the **CosmicDuke** toolset was compiled on the 16th of January 2010. Back then, **CosmicDuke** still lacked most of the credential-stealing functionality found in later samples. We believe that during the spring of 2010, the credential and file stealing capabilities of **PinchDuke** were slowly ported to **CosmicDuke**, effectively making **PinchDuke** obsolete.

During this period of transition, **CosmicDuke** would often embed **PinchDuke** so that, upon execution, **CosmicDuke** would write to disk and execute **PinchDuke**. Both **PinchDuke** and **CosmicDuke** would then operate independently on the same compromised host, including performing separate information gathering, data exfiltration and communication with a command and control (C&C) server - although both malware would often use the same C&C server. We believe the purpose of this parallel use was to 'fieldtest' the new **CosmicDuke** tool, while at the same time ensuring operational success with the tried-and-tested **PinchDuke**.

During this period of **CosmicDuke** testing and development, the Duke authors also started experimenting with the use of privilege escalation vulnerabilities. Specifically, on the 19th of January 2010 Tavis Ormandy disclosed a local privilege escalation vulnerability (CVE-2010-0232) affecting Microsoft Windows. As part of the disclosure, Ormandy also included the source code for a proof-of-concept exploit for the vulnerability [5]. Just 7 days later, on the 26th of January, a component for **CosmicDuke** was compiled that exploited the vulnerability and allowed the tool to operate with higher privileges.

One loader to load them all (almost)

In addition to all the other components being produced by the Dukes group, in 2010 they were also actively developing and testing a new *loader* - a component that wraps the core malware code and provides an additional layer of obfuscation.

The first sample of this loader was compiled on the 26th of July 2010, making it a direct predecessor of what has since become known as the "MiniDuke loader", as later versions were extensively used by both MiniDuke and CosmicDuke.

Some hints about the history of the "MiniDuke loader" were noted in the CosmicDuke whitepaper we published[6] in 2014, where we observed that the loader appeared to have been in use with CosmicDuke before it was used with MiniDuke. In fact, we now know that before being used with either, the "MiniDuke loader" was used to load PinchDuke. The first known sample of the loader was used during the summer of 2010, while the most recent samples were seen during the spring of 2015.

This neatly ties together many of the tools used by the Dukes group, as versions of this one loader have been used to load malware from three different Dukes-related toolsets – CosmicDuke, PinchDuke, and MiniDuke – over the course of five years.

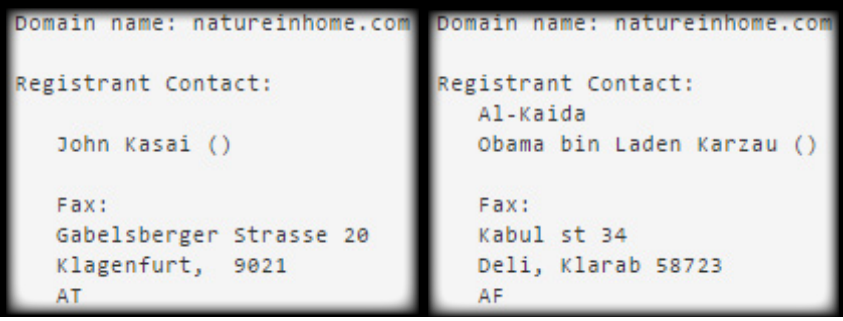


IMAGE 2: COMPARING WHOIS REGISTRATION DETAILS

Original whois registration details (left) for natureinhome.com, one of the Duke command & control server domains registered on the 29th of January, 2011, to "John Kasai". Details for the domain were later changed (right), providing a small glimpse of the Dukes group's sense of humor.

2011: John Kasai of Klagenfurt, Austria

During 2011, the Dukes appear to have significantly expanded both their arsenal of malware toolsets and their C&C infrastructure. While the Dukes employed both hacked websites and purposely rented servers for their C&C infrastructure, the group rarely registered their own domain names, preferring instead to connect to their self-operated servers via IP addresses.

The beginning of 2011 however saw a significant break from that routine, when a large grouping of domain names was registered by the Dukes in two batches; the first batch was registered on the 29th of January and the second on the 13th of February. The domains in this second group were all initially registered with the same alias: "John Kasai of Klagenfurt, Austria" (image 2, above). These domains were used by the Dukes in campaigns involving many of their different malware toolsets all the way until 2014. Like the "MiniDuke loader", these "John Kasai" domains also provide a common thread tying together much of the tools and infrastructure of the Dukes.

2011: Continuing expansion of the Dukes arsenal

By 2011, the Dukes had already developed at least 3 distinct malware toolsets, including a plethora of supporting components such as loaders and persistence modules. In fact, as a sign of their arsenal's breadth, they had already decided to retire one of these malware toolsets as obsolete after developing a replacement for it, seemingly from scratch.

The Dukes continued the expansion of their arsenal in 2011 with the addition of two more toolsets: **MiniDuke** and **CozyDuke**. While all of the earlier toolsets – **GeminiDuke**, **PinchDuke**, and **CosmicDuke** – were designed around a core infostealer component, **MiniDuke** is centered on a simplistic backdoor component whose purpose is to enable the remote execution of commands on the compromised system. The first observed samples of the **MiniDuke** backdoor component are from May 2011. This backdoor component however is technically very closely related to **GeminiDuke**, to the extent that we believe them to share parts of their source code. The origins of **MiniDuke** can thus be traced back to the origins of **GeminiDuke**, of which the first observed sample was compiled in January of 2009.

Unlike the simplistic **MiniDuke** toolset, **CozyDuke** is a highly versatile, modular, malware "platform" whose functionality lies not in a single core component but in an array of modules that toolset may be instructed to download from its C&C server. These modules can be are used to selectively provide **CozyDuke** with just the functionality deemed necessary for the mission at hand. **CozyDuke's** modular platform approach is a clear break from the designs of the previous Duke toolsets.

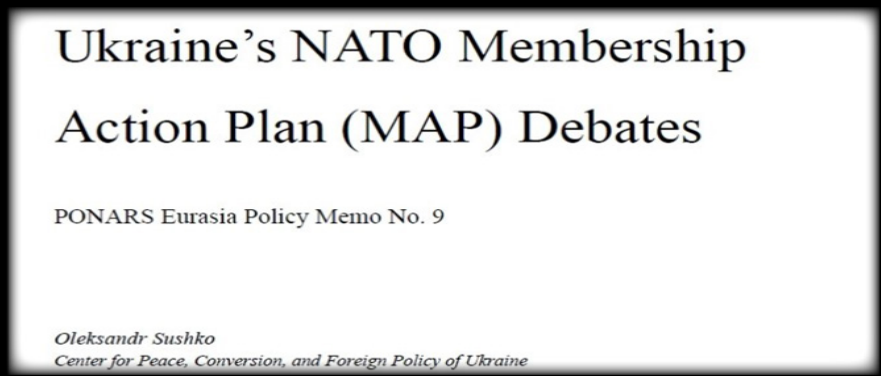
The stylistic differences between **CozyDuke** and its older siblings are further exemplified by the way it was coded. All of the 4 previously mentioned toolsets were written in a minimalistic style commonly seen with malware; **MiniDuke** even goes as far as having many components written in Assembly language. **CozyDuke** however represents the complete opposite. Instead of being written in Assembly or C, it was written in C++ , which provides added layers of abstraction for the developer's perusal, at the cost of added complexity.

Contrary to what might be expected from malware, early **CozyDuke** versions also lacked any attempt at obfuscating or hiding their true nature. In fact, they were extremely open and verbose about their functionality - for example, early samples contained a plethora of logging messages in unencrypted form. In comparison, even the earliest known **GeminiDuke** samples encrypted any strings that might have given away the malware's true nature.

Finally, early **CozyDuke** versions also featured other elements that one would associate more with a traditional software development project than with malware. For instance, the earliest known **CozyDuke** version utilized a feature of the Microsoft Visual C++ compiler known as *run-time error checking*. This feature added automatic error checking to critical parts of the program's execution at the cost, from a malware perspective, of providing additional hints that make the malware's functionality easier for reverse engineers to understand.

IMAGE 3: DECOY DOCUMENT

One of the Ukraine-themed decoy document used during a MiniDuke campaign in February 2013


Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine

Based on these and other similar stylistic differences observed between **CozyDuke** and its older siblings, we speculate that while the older Duke families appear to be the work of someone with a background in malware writing (or at the least in hacking), **CozyDuke**'s author or authors more likely came from a software development background.

2012: Hiding in the shadows

We still know surprisingly few specifics about the Dukes group's activities during 2012. What we do know is that, based on the samples of Duke malware that we were able to recover from 2012, the Dukes appear to have continued actively using and developing all of their tools. Of these, **CosmicDuke** and **MiniDuke** appear to have been in more active use, while receiving only minor updates. **GeminiDuke** and **CozyDuke** on the other hand appear to have been less used in actual operations, but did undergo much more significant development.

2013: MiniDuke flies too close to the sun

On the 12th of February 2013, FireEye published a blogpost[7] alerting readers to a combination of new Adobe Reader 0-day vulnerabilities, CVE-2013-0640 and CVE-2013-0641, that were being actively exploited in the wild. 8 days after FireEye's initial alert, Kaspersky spotted the same exploit being used to spread an entirely different malware family from the one mentioned in the original report. On 27th February, Kaspersky[8] and CrySyS[9] Lab published research on this previously unidentified malware family, dubbing it **MiniDuke**.

As we now know, by February 2013 the Dukes group had been operating **MiniDuke** and other toolsets for at least 4 and a half years. Their malware had not stayed undetected for those 4 and a half years. In fact, in 2009 a **PinchDuke** sample had been included in the malware set used by the AV-Test security product testing organization to perform anti-virus product comparison reviews. Until 2013 however, earlier Duke toolsets had not been put in a proper context. That finally started to change in 2013.

The **MiniDuke** samples that were spread using these exploits were compiled on the 20th of February, after the exploit was already publicly known. One might argue that since this took place after the exploits were publicly mentioned, the Dukes simply copied them. We however do not believe so. As mentioned by Kaspersky, even though the exploits used for these **MiniDuke** campaigns were near-identical to those described by FireEye, there were nevertheless small differences. Of these, the crucial one is the presence of PDB strings in the **MiniDuke** exploits. These strings, which are generated by the compiler when using specific compilation settings, means that the components of the exploits used with **MiniDuke** had to have been compiled independently from those described by FireEye.

We do not know whether the Dukes compiled the components themselves or whether someone else compiled the components before handing them to the group. This does however still rule out the possibility that the Dukes simply obtained copies of the exploit binaries described by FireEye and repurposed them.

In our opinion, this insistence on using exploits that are already under heightened scrutiny suggests the existence of at least one of three circumstances. Firstly, the Dukes may have been confident enough in their own abilities (and in the slowness of their opponents to react to new threats) that they did not care if their targets may already be on the lookout for anyone exploiting these vulnerabilities. Secondly, the value the Dukes intended to gain from these **MiniDuke** campaigns may have been so great that they deemed it worth the risk of getting noticed. Or thirdly, the Dukes may have invested so much into these campaigns that by the time FireEye published their blogpost, the Dukes felt they could not afford to halt the campaigns.

We believe all three circumstances to have coexisted at least to some extent. As will become evident in this report, this was not a one-off case but a recurring theme with the Dukes, in that they would rather continue with their operations as planned than retreat from operating under the spotlight.

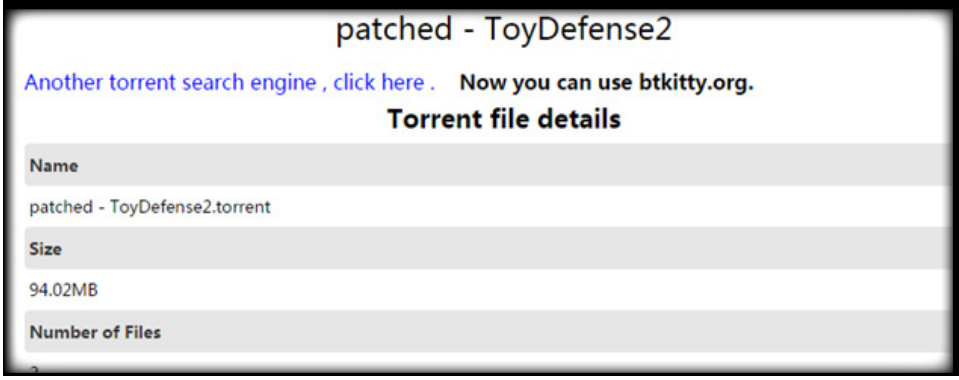


IMAGE 4: ONIONDUKE-TROJANIZED TORRENT FILE

Example of a torrent file containing an executable trojanized with the OnionDuke toolset

As originally detailed in Kaspersky's whitepaper, the **MiniDuke** campaigns from February 2013 employed spear-phishing emails with malicious PDF file attachments. These PDFs would attempt to silently infect the recipient with **MiniDuke,** while distracting them by displaying a decoy document. The headings of these documents included "Ukraine's NATO Membership Action Plan (MAP) Debates", "The Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights", and "Ukraine's Search for a Regional Foreign Policy" (image 3, page 8). The targets of these campaigns, according to Kaspersky, were located variously in Belgium, Hungary, Luxembourg and Spain [8].

Kaspersky goes on to state that by obtaining log files from the **MiniDuke** command and control servers, they were able to identify high-profile victims from Ukraine, Belgium, Portugal, Romania, the Czech Republic, Ireland, the United States and Hungary [8].

2013: The curious case of OnionDuke

After the February campaigns, **MiniDuke** activity appeared to quiet down, although it did not fully stop, for the rest of 2013. The Dukes group as a whole however showed no sign of slowing down. In fact, we saw yet another Duke malware toolset, **OnionDuke**, appear first in 2013. Like **CozyDuke**, **OnionDuke** appears to have been designed with versatility in mind, and takes a similarly modular platform approach. The **OnionDuke** toolset includes various modules for purposes such as password stealing, information gathering, denial of service (DoS) attacks, and even posting spam to the Russian social media network, VKontakte. The **OnionDuke** toolset also includes a dropper, an information stealer variant and multiple distinct versions of the core component that is responsible for interacting with the various modules.

What makes **OnionDuke** especially curious is an infection vector it began using during the summer of 2013. To spread the toolset, the Dukes used a *wrapper* to combine **OnionDuke** with legitimate applications, created torrent files containing these trojanized applications, then uploaded them to websites hosting torrent files (image 4, above). Victims who used the torrent files to download the applications would end up getting infected with **OnionDuke**.

For most of the **OnionDuke** components we observed, the first versions that we are aware of were compiled during the summer of 2013, suggesting that this was a period of active development around this toolset. Critically however, the first sample of the **OnionDuke** dropper, which we observed being used only with components of this toolset, was compiled on the 17th of February 2013. This is significant because it suggests that **OnionDuke** was under development before any part of the Duke operation became public. **OnionDuke's** development therefore could not have been simply a response to the outing of one of the other Duke malware, but was instead intended for use alongside the other toolsets. This indication that the Dukes planned to use an arsenal of 5 malware toolsets in parallel suggests that they were operating with both significant resources and capacity.

2013: The Dukes and Ukraine

In 2013, many of the decoy documents employed by the Dukes in their campaigns were related to Ukraine; examples include a letter undersigned by the First Deputy Minister for Foreign Affairs of Ukraine, a letter from the embassy of the Netherlands in Ukraine to the Ukrainian Ministry of Foreign affairs and a document titled "Ukraine's Search for a Regional Foreign Policy". [10]

These decoy documents however were written before the start of the November 2013 Euromaidan protests in Ukraine and the subsequent upheaval. It is therefore important to note that, contrary to what might be assumed, we have actually observed a drop instead of an increase in Ukraine-related campaigns from the Dukes following the country's political crisis.

This is in stark contrast to some other suspected Russian threat actors (such as Operation Pawn Storm [11]) who appear to have increased their targeting of Ukraine following the crisis. This supports our analysis that the overarching theme in the Dukes' targeting is the collection of intelligence to support diplomatic efforts. The Dukes actively targeted Ukraine before the crisis, at a time when Russia was still weighing her options, but once Russia moved from diplomacy to direct action, Ukraine was no longer relevant to the Dukes in the same way.

10

2013: CosmicDuke's war on drugs

In a surprising turn of events, in September 2013 a **CosmicDuke** campaign was observed targeting Russian speakers involved in the trade of illegal and controlled substances.

Kaspersky Labs, who sometimes refer to **CosmicDuke** as 'Bot Gen Studio', speculated that "one possibility is that 'Bot Gen Studio' is a malware platform also available as a so-called 'legal spyware' tool"; therefore, those using **CosmicDuke** to target drug dealers and those targeting governments are two separate entities [12]. We however feel it is unlikely that the **CosmicDuke** operators targeting drug dealers and those targeting governments could be two entirely independent entities. A shared supplier of malware would explain the overlap in tools, but it would not explain the significant overlap we have also observed in operational techniques related to command and control infrastructure. Instead, we feel the targeting of drug dealers was a new task for a subset of the Dukes group, possibly due to the drug trade's relevance to security policy issues. We also believe the tasking to have been temporary, because we have not observed any further similar targeting from the Dukes after the spring of 2014.

2014: MiniDuke's rise from the ashes

While **MiniDuke** activity quieten down significantly during the rest of 2013 following the attention it garnered from researchers, the beginning of 2014 saw the toolset back in full force. All **MiniDuke** components, from the loader and downloader to the backdoor, had been slightly updated and modified during the downtime. Interestingly, no significant new functionality was added during these modifications, suggesting that the primary purpose of the updates was an attempt to regain the element of stealth and undetectability that had been lost almost a year earlier.

Of these modifications, the most important were the ones done to the loader. These resulted in a loader version that would later become known as the "Nemesis Gemina loader" due to PDB strings found in many of the samples. It is however still only an iteration on earlier versions of the **MiniDuke** loader. The first observed samples of the Nemesis Gemina loader (compiled on 14th December 2013) were used to load the updated **MiniDuke** backdoor, but by the spring of 2014 the Nemesis Gemina loader was also observed in use with **CosmicDuke**.

2014: CosmicDuke's moment of fame and the scramble that ensued

Following the MiniDuke expose, **CosmicDuke** in turn got its moment of fame when F-Secure published a whitepaper about it on 2nd July 2014 [6]. The next day, Kaspersky also published their own research on the malware [12]. It should be noted that until this point, even though **CosmicDuke** had been in active use for over 4 years, and had undergone minor modifications and updates during that time, even the most recent **CosmicDuke** samples would often embed persistence components that date back to 2012. These samples would also contain artefacts of functionality from the earliest **CosmicDuke** samples from 2010.

It is therefore valuable to observe how the Dukes reacted to **CosmicDuke's** outing at the beginning of July. By the end of that month, **CosmicDuke** samples we found that had been compiled on the 30th of July had removed unused parts of toolset that had essentially just been relics of the past. Similarly, some of the hardcoded values that had remained unaltered in **CosmicDuke** samples for many years were changed. We believe these edits were an attempt at evading detection by modifying or removing parts of the toolset that the authors believed might be helpful in identifying and detecting it.

Concurrently with the alterations to **CosmicDuke**, the Dukes were also hard at work modifying their trusted loader. Much like the toolset itself, the loader used by both **MiniDuke** and **CosmicDuke** had previously only undergone one major update (the Nemesis Gemina upgrade) since the first known samples from 2010. Again, much of the modification work focused on removing redundant code in an attempt to appear different from earlier versions of the loader. Interestingly however, another apparent evasion trick was also attempted - forging of the loaders' compilation timestamps.

the first **CosmicDuke** sample we observed after its outing was a sample compiled on the 30th of July 2014. The loader used by the sample purported to have been compiled on the 25th of March 2010. Due to artefacts left in the loader during compilation time however, we know that the it used a specific version of the Boost library, 1.54.0, that was only published on the 1st of July 2013 [13]. The compilation timestamp therefore had to have been faked. F-Secure's whitepaper[6] on **CosmicDuke** includes a timeline of the loader's usage, based on compilation timestamps. Perhaps the Dukes group thought that by faking a timestamp from before the earliest one cited in the whitepaper, they might be able to confuse researchers.

IMAGE 5: MORE DECOYS

US letter fax test decoy (left) and screenshot of the monkey video decoy (right) used at various times by CozyDuke

During the rest of 2014 and the spring of 2015, the Dukes continued making similar evasion-focused modifications to **CosmicDuke**, as well as experimenting with ways to obfuscate the loader. In the latter case however, the group appear to have also simultaneously developed an entirely new loader, which we first observed being used in conjunction with **CosmicDuke** during the spring of 2015.

While it is not surprising that the Dukes reacted to multiple companies publishing extensive reports on one of their key toolsets, it is valuable to note the manner in which they responded. Much like the **MiniDuke** expose in February 2013, the Dukes again appeared to prioritize continuing operations over staying hidden. They could have ceased all use of **CosmicDuke** (at least until they had developed a new loader) or retired it entirely, since they still had other toolsets available. Instead, they opted for minimal downtime and attempted to continue operations, with only minor modifications to the toolset.

2014: CozyDuke and monkey videos

While we now know that **CozyDuke** had been under development since at least the end of 2011, it was not until the early days of July 2014 that the first large-scale **CozyDuke** campaign that we are aware of took place. This campaign, like later **CozyDuke** campaigns, began with spear-phishing emails that tried to impersonate commonly seen spam emails. These spear-phishing emails would contain links that eventually lead the victim to becoming infected with **CozyDuke**.

Some of the early spear-phishing emails from the July campaign were efax-themed and used the same "US letter fax test page" decoy document that was used a year later by **CloudDuke**. In at least one case however, the email instead contained a link to a zip-archive file named "Office Monkeys LOL Video.zip", which was hosted on the DropBox cloud storage service. What made this particular case interesting was that instead of the usual dull PDF file, the decoy was a Flash video file, more specifically a Super Bowl advertisement from 2007 purporting to show monkeys at an office (image 5, above).

2014: OnionDuke gets caught using a malicious Tor node

On the 23rd of October 2014, Leviathan Security Group published a blog post describing a malicious Tor exit node they had found. They noted that this node appeared to be maliciously modifying any executables that were downloaded through it over a HTTP connection. Executing the modified applications obtained this way would result in the victim being infected with unidentified malware. On the 14th of November, F-Secure published a blog post naming the malware **OnionDuke** and associating it with **MiniDuke** and **CosmicDuke**, the other Duke toolsets known at the time [14].

Based on our investigations into **OnionDuke**, we believe that for about 7 months, from April 2014 to when Leviathan published their blog post in October 2014, the Tor exit node identified by the researchers was being used to wrap executables on-the-fly with **OnionDuke** (image 6, page 13). This is similar to the way in which the toolset was being spread via trojanized applications in torrent files during the summer of 2013.

While investigating the **OnionDuke** variant being spread by the malicious Tor node, we also identified another **OnionDuke** variant that appeared to have successfully compromised multiple victims in the ministry of foreign affairs of a European country during the spring of 2014. This variant differed significantly in functionality from the one being spread via the Tor node, further suggesting that different **OnionDuke** variants are intended for different kinds of victims.

We believe that, unusually, the purpose of the **OnionDuke** variant spread via the Tor node was not to pursue targeted attacks but instead to form a small botnet for later use. This **OnionDuke** variant is related to the one seen during the summer of 2013 being spread via torrent files. Both of these infection vectors are highly diffuse or untargeted when compared to spear-phishing, the usual infection vector of choice for the Dukes.

Further, the functionality of the **OnionDuke** variant is derived from a number of modules. While one of these modules gathers system information and another attempts to steal the victim's usernames and passwords, as one would expect from a malware used for a targeted attack, the other two known **OnionDuke** modules are quite the opposite; one is designed for use in DoS attacks and the other for posting predetermined messages to the Russian VKontakte social media site. This sort of functionality is more common in criminality-oriented botnets, not state-sponsored targeted attacks.

We have since been able to identify at least two separate **OnionDuke** botnets. We believe the formation of the first of these botnets began in January 2014, using both unidentified infection vectors and the known malicious Tor node, and continued until our blogpost was published in November. We believe the formation of the second botnet began in August 2014 and continued until January 2015. We have been unable to identify the infection vectors used for this second botnet, but the C&C servers it uses has open directory listings, allowing us to retrieve files containing listings of victim IP addresses. The geographic distribution of these IP addresses (image 7, page 13) further supports our theory that the purpose of this **OnionDuke** variant was not targeted attacks against high-profile targets.

One theory is that the botnets were a criminal side business for the Dukes group. The size of the botnet however (about 1400 bots) is very small if its intended use is for commercial DoS attacks or spam-sending. Alternatively, **OnionDuke** also steals user credentials from its victims. providing another potential revenue source. The counter to that argument however is that the value of stolen credentials from users in the countries with the highest percentage of **OnionDuke** bots (Mongolia and India) are among the lowest on underground markets.

2015: The Dukes up the ante

The end of January 2015 saw the start of the most high-volume Duke campaign seen thus far, with thousands of recipients being sent spear-phishing emails that contained links to compromised websites hosting **CozyDuke**. Curiously, the spear-phishing emails were strikingly similar to the e-fax themed spam usually seen spreading ransomware and other common crimeware. Due to the sheer number of recipients, it may not have been possible to customize the emails in the same way as was possible with lower-volume campaigns.

The similarity to common spam may however also serve a more devious purpose. It is easy to imagine a security analyst, burdened by the amount of attacks against their network, dismissing such common-looking spam as "just another crimeware spam run", allowing the campaign to, in essence, hide in the masses [15]. The **CozyDuke** activity continues one of the long-running trends of the Dukes operations, the use of multiple malware toolsets against a single target. In this case, the Dukes first attempted to infect large numbers of potential targets with **CozyDuke** (and in a more obvious manner than previously seen). They would then use the toolset to gather initial information on the victims, before deciding which ones to pursue further. For the victims deemed interesting enough, the Dukes would deploy a different component.

We believe the primary purpose of this tactic is an attempt at evading detection in the targeted network. Even if the noisy initial **CozyDuke** campaign is noticed by the victim organization, or by someone else who then makes it publicly known, defenders will begin by first looking for indicators of compromise (IOCs) related to the **CozyDuke** toolset. If however by that time the Dukes are already operating within the victim's network, using an another toolset with different IOCs, then it is reasonable to assume that it will take much longer for the victim organization to notice the infiltration.

In previous cases, the group used their malware toolsets interchangeably, as either the initial or a later-stage toolset in a campaign. For these **CozyDuke** campaigns however, the Dukes appear to have employed two particular later-stage toolsets, **SeaDuke** and **HammerDuke**, that were purposely designed to leave a persistent backdoor on the compromised network. **HammerDuke** is a set of backdoors that was first seen in the wild in February 2015, while **SeaDuke** is a cross-platform backdoor that was, according to Symantec, first spotted in the wild in October 2014 [16]. Both toolsets were originally spotted being deployed by **CozyDuke** to its victims.

What makes **SeaDuke** special is that it was written in Python and designed to work on both Windows and Linux systems; it is the first cross-platform tool we have seen from the Dukes. One plausible reason for developing such a flexible malware might be that the group were increasingly encountering victim environments where users were using Linux as their desktop operating system.

Meanwhile, **HammerDuke** is a Windows-only malware (written in .NET) and comes in two variants. The simpler one will connect to a hardcoded C&C server over HTTP or HTTPS to download commands to execute. The more advanced variant, on the other hand, will use an algorithm to generate a periodically-changing Twitter account name and will then attempt to find tweets from that account containing links to the actual download location of the commands to execute. In this way, the advanced **HammerDuke** variant attempts to hide its network traffic in more legitimate use of Twitter. This method is not unique to **HammerDuke**, as **MiniDuke**, **OnionDuke**, and **CozyDuke** all support similar use of Twitter to retrieve links to additional payloads or commands.

IMAGE 6: FLOWCHART OF HOW ONIONDUKE USES MALICIOUS TOR NODE TO INFECT VICTIMS

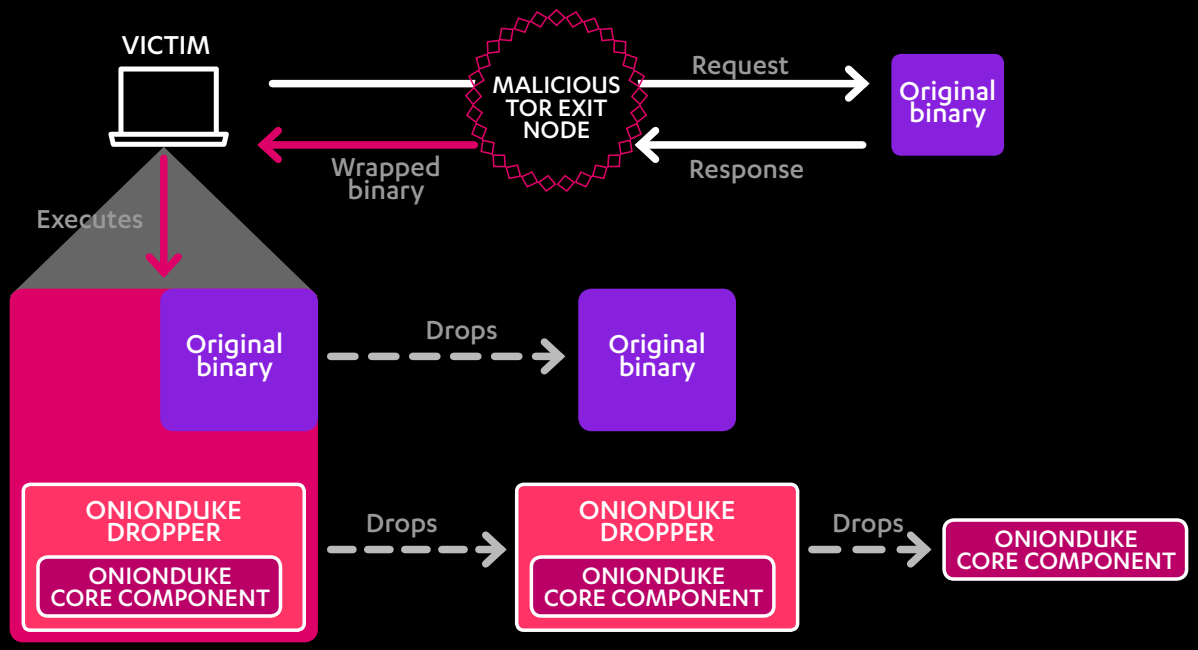
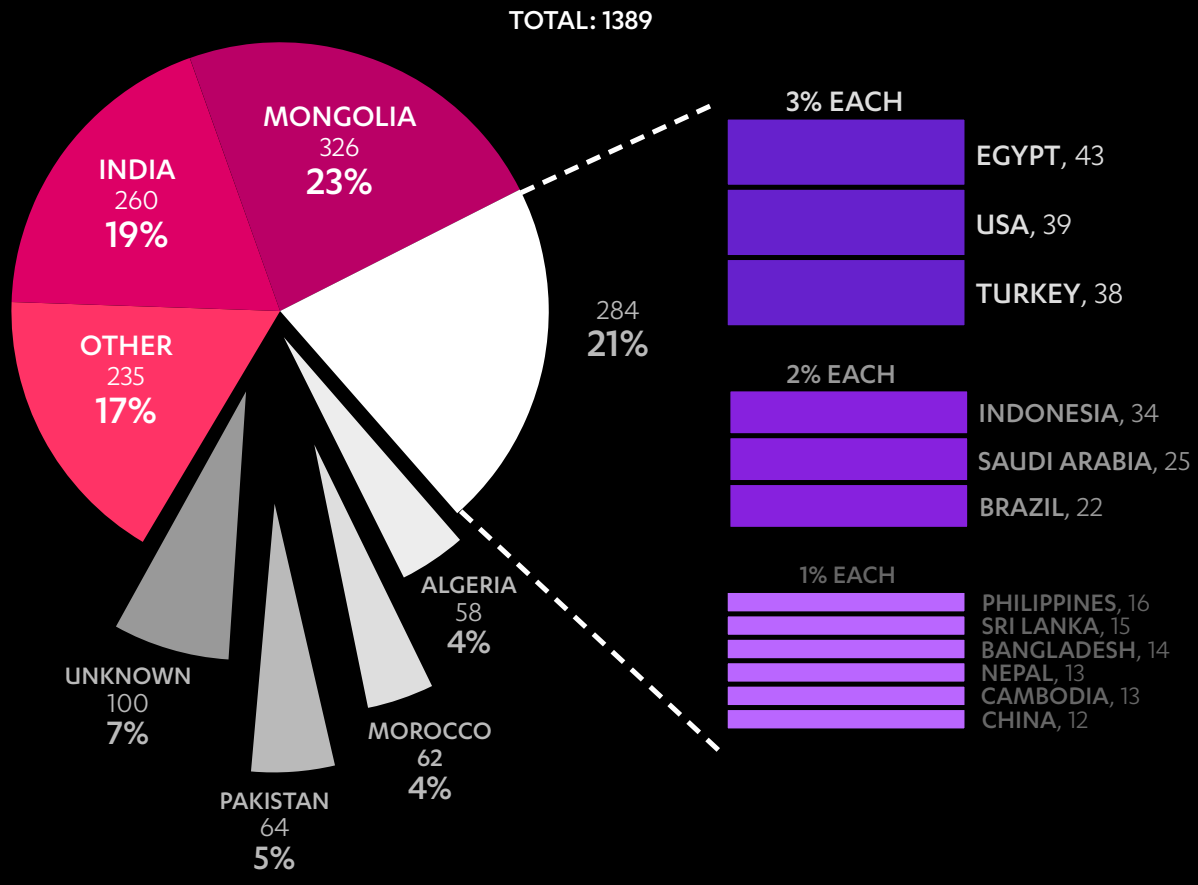


IMAGE 7: GEOGRAPHICAL DISTRIBUTION OF ONIONDUKE BOTNET



2015: CloudDuke

In the beginning of July 2015, the Dukes embarked on yet another large-scale phishing campaign. The malware toolset used for this campaign was the previously unseen **CloudDuke** and we believe that the July campaign marks the first time that this toolset was deployed by the Dukes, other than possible small-scale testing.

The **CloudDuke** toolset consists of at least a loader, a downloader, and two backdoors variants. Both backdoors (internally referred to by their authors as "BastionSolution" and "OneDriveSolution") essentially allow the operator to remotely execute commands on the compromised machine. The way in which each backdoor does so however is significantly different. While the BastionSolution variant simply retrieves commands from a hard-coded C&C server controlled by the Dukes, the OneDriveSolution utilizes Microsoft's OneDrive cloud storage service for communicating with its masters, making it significantly harder for defenders to notice the traffic and block the communication channel.

What is most significant about the July 2015 **CloudDuke** campaign is the timeline. The campaign appeared to consist of two distinct waves of spear-phishing, one during the first days of July and the other starting from the 20th of the month. Details of the first wave, including a thorough technical analysis of **CloudDuke**, was published by Palo Alto Networks on 14th July [17]. This was followed by additional details from Kaspersky in a blog post published on 16th July [18].

Both publications happened before the second wave took place and received notable publicity. Despite the attention and public exposure of the toolset's technical details (including IOCs) to defenders, the Dukes still continued with their second wave of spear-phishing, including the continued use of **CloudDuke**. The group did change the contents of the spear-phishing emails they sent, but they didn't switch to a new email format; instead, they reverted to the same efax-themed format that they had previously employed, even to the point of reusing the exact same decoy document that they had used in the **CozyDuke** campaign a year earlier (July 2014).

This once more highlights two crucial behavioral elements of the Dukes group. Firstly, as with the **MiniDuke** campaigns of February 2013 and **CosmicDuke** campaigns in the summer of 2014, again the group clearly prioritized the continuation of their operations over maintaining stealth. Secondly, it underlines their boldness, arrogance and self-confidence; they are clearly confidence in both their ability to compromise their targets even when their tools and techniques are already publicly known, and critically, they appear to be extremely confident in their ability to act with impunity.

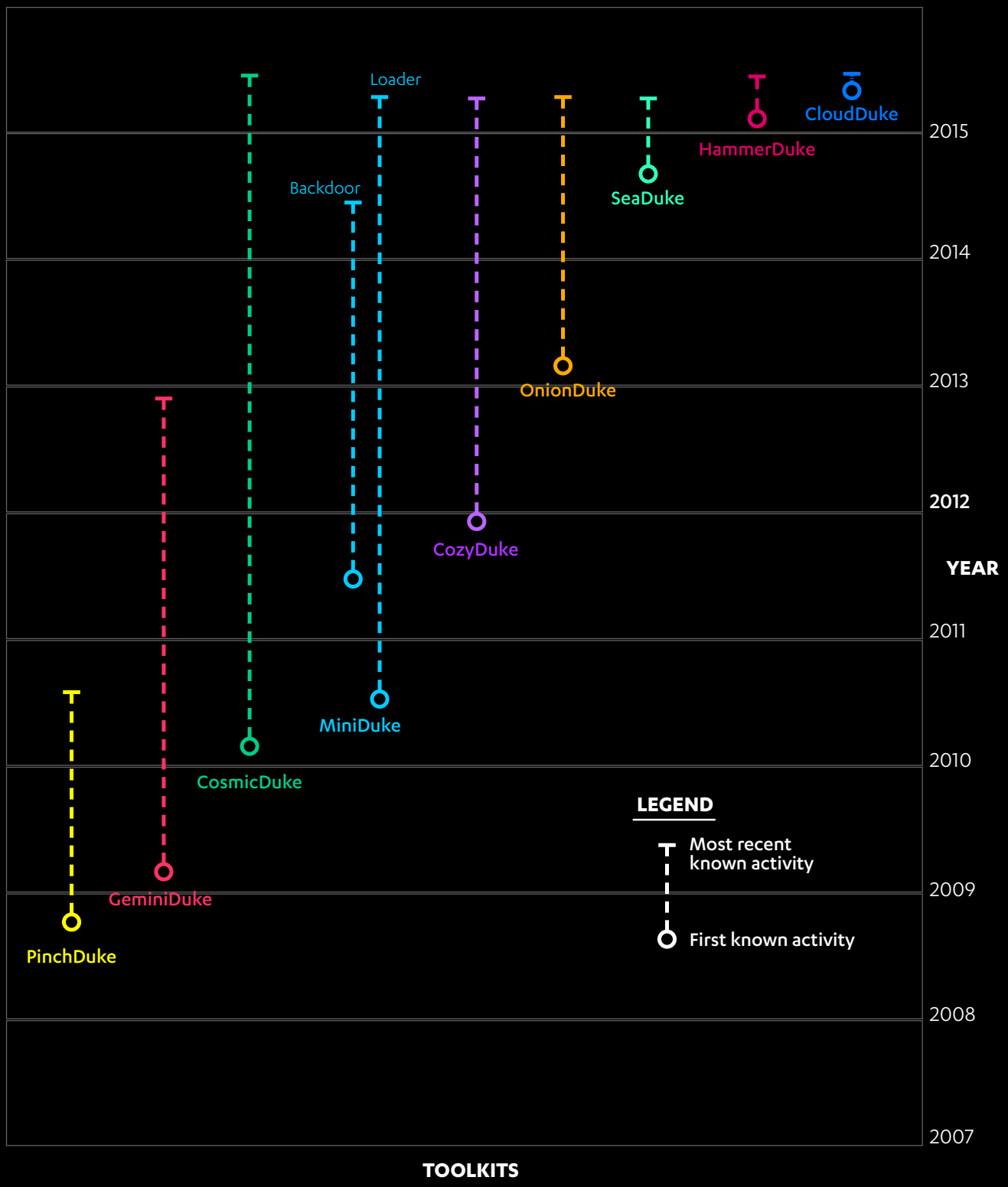
2015: Continuing surgical strikes with CosmicDuke

In addition to the notably overt and large-scale campaigns with **CozyDuke** and **CloudDuke**, the Dukes also continued to engage in more covert, surgical campaigns using **CosmicDuke**. The latest of these campaigns that we are aware of occurred during the spring and early summer of 2015. As their infection vectors, these campaigns used malicious documents exploiting recently fixed vulnerabilities.

Two of these campaigns were detailed in separate blog posts by the Polish security company Prevenity, who said that both campaigns targeted Polish entities with spear-phishing emails containing malicious attachments with relevant Polish language names [19] [20]. A third, similar, **CosmicDuke** campaign was observed targeting Georgian entities and using an attachment with a Georgian-language name that translates to "NATO consolidates control of the Black Sea.docx".

Based on this, we do not believe that the Dukes are replacing their covert and targeted campaigns with the overt and opportunistic **CozyDuke** and **CloudDuke** style of campaigns. Instead, we believe that they are simply expanding their acitivities by adding new tools and techniques.

TIMELINE OF KNOWN ACTIVITY FOR THE VARIOUS DUKE TOOLKITS



TOOLS AND TECHNIQUES OF THE DUKES

PINCHDUKE

First known activity:	November 2008
Most recent known activity:	Summer 2010
Other names:	N/A
C&C communication methods:	HTTP (S)
Known toolset components:	◊ Multiple loaders ◊ information stealer

The PinchDuke toolset consists of multiple loaders and a core information stealer trojan. The loaders associated with the PinchDuke toolset have also been observed being used with CosmicDuke.

The PinchDuke information stealer gathers system configuration information, steals user credentials, and collects user files from the compromised host transferring these via HTTP(S) to a C&C server. We believe PinchDuke's credential stealing functionality is based on the source code of the Pinch credential stealing malware (also known as LdPinch) that was developed in the early 2000s and has later been openly distributed on underground forums.

Credentials targeted by PinchDuke include ones associated with the following software or services:

- The Bat!
- Yahoo!
- Mail.ru
- Passport.Net
- Google Talk
- Netscape Navigator
- Mozilla Firefox
- Mozilla Thunderbird
- Internet Explorer
- Microsoft Outlook
- WinInet Credential Cache
- LDAP

PinchDuke will also search for files that have been created within a predefined timeframe and whose file extension is present in a predefined list.

As a curiosity, most PinchDuke samples contain a Russian language error message,

"Ошибка названия модуля! Название секции данных должно быть 4 байта!"

which roughly translates to:

"There is an error in the module's name! The length of the data section name must be 4 bytes!"

GEMINIDUKE

First known activity:	January 2009
Most recent known activity:	December 2012
Other names:	N/A
C&C communication methods:	HTTP (S)
Known toolset components:	◊ Loader ◊ information stealer ◊ Multiple persistence components

The GeminiDuke toolset consists of a core information stealer, a loader and multiple persistence-related components. Unlike CosmicDuke and PinchDuke, GeminiDuke primarily collects information on the victim computer's configuration. The collected details include:

- Local user accounts
- Network settings
- Internet proxy settings
- Installed drivers
- Running processes
- Programs previously executed by users
- Programs and services configured to automatically run at startup
- Values of environment variables
- Files and folders present in any users home folder
- Files and folders present in any users My Documents
- Programs installed to the Program Files folder
- Recently accessed files, folders and programs

As is common for malware, the GeminiDuke infostealer uses a mutex to ensure that only one instance of itself is running at a time. What is less common is that the name used for the mutex is often a timestamp. We believe these timestamps to be generated during the compilation of GeminiDuke from the local time of the computer being used, and always reference the time in the UTC+0 timezone.

Comparing the GeminiDuke compilation timestamps with the local time timestamps used as mutex names, and adjusting for the presumed timezone difference, we note that all of the mutex names reference a time and date that is within seconds of the respective sample's compilation timestamp. Additionally, the apparent timezone of the timestamps in all of the GeminiDuke samples compiled during the winter is UTC+3, while for samples compiled during the summer, it is UTC+4.

The observed timezones correspond to the pre-2011 definition of Moscow Standard Time (MSK) [21], which was UTC+3 during the winter and UTC+4 during the summer. In 2011 MSK stopped following Daylight Saving Time (DST) and was set to UTC+4 year-round, then reset to UTC +3 year-round in 2014. Some of the observed GeminiDuke samples that used timestamps as mutex names were compiled while MSK still respected DST and for these samples, the timestamps perfectly align with MSK as it was defined at the time.

Map of timezones in Russia; © Eric Muller
Pink: MSK (UTC +3) ; Orange: UTC +4

However, GeminiDuke samples compiled after MSK was altered still vary the timezone between UTC+3 in the winter and UTC+4 during the summer. While computers using Microsoft Windows automatically adjust for DST, changes in timezone definitions require that an update to Windows be installed. We therefore believe that the Dukes group simply failed to update the computer they were using to compile GeminiDuke samples, so that the timestamps seen in later samples still appear to follow the old definition of Moscow Standard Time.

The GeminiDuke infostealer has occasionally been wrapped with a loader that appears to be unique to GeminiDuke and has never been observed being used with any of the other Duke toolsets. GeminiDuke also occasionally embeds additional executables that attempt to achieve persistence on the victim computer. These persistence components appear to be uniquely customized for use with GeminiDuke, but they use many of the same techniques as CosmicDuke persistence components.

COSMICDUKE

First known activity:	January 2010
Most recent known activity:	Summer 2015
Other names:	Tinybaron, BotgenStudios, NemesisGemina
C&C communication methods:	HTTP (S), FTP, WebDav
Known toolset components:	◊ Information stealer ◊ Privilege escalation component ◊ Multiple persistence components

The CosmicDuke toolset is designed around a main information stealer component. This information stealer is augmented by a variety of components that the toolset operators may selectively include with the main component to provide additional functionalities, such as multiple methods of establishing persistence, as well as modules that attempt to exploit privilege escalation vulnerabilities in order to execute CosmicDuke with higher privileges.

CosmicDuke's information stealing functionality includes:

- Keylogging
- Taking screenshots
- Stealing clipboard contents
- Stealing user files with file extensions that match a predefined list
- Exporting the users cryptographic certificates including private keys
- Collecting user credentials, including passwords, for a variety of popular chat and email programs as well as from web browsers

CosmicDuke may use HTTP, HTTPS, FTP or WebDav to exfiltrate the collected data to a hardcoded C&C server.

While we believe CosmicDuke to be an entirely custom-written toolset with no direct sharing of code with other Duke toolsets, the high-level ways in which many of its features have been implemented appear to be shared with other members of the Duke arsenal.

Specifically, the techniques CosmicDuke uses to extract user credentials from targeted software and to detect the presence of analysis tools appear to be based on the techniques used by PinchDuke. Likewise, many of CosmicDuke's persistence components use techniques also used by components associated with GeminiDuke and CozyDuke. In all of these cases, though the techniques are the same, but the code itself has been altered to work with the toolset in question, leading to small differences in the final implementation.

A few of the CosmicDuke samples we discovered also included components that attempt to exploit either of the publicly known CVE-2010-0232 or CVE-2010-4398 privilege escalation vulnerabilities. In the case of CVE-2010-0232, the exploit appears to be based directly on the proof of concept code published by Tavis Ormandy when he disclosed the vulnerability [5]. We believe that the exploit for CVE-2010-4398 was also based on a publicly available proof of concept [22].

In addition to often embedding persistence or privilege escalation components, CosmicDuke has occasionally embedded PinchDuke, GeminiDuke, or MiniDuke components. It should be noted that CosmicDuke does not interoperate with the second, embedded malware in any way other than by writing the malware to disk and executing it. After that, CosmicDuke and the second malware operate entirely independently of each other, including separately contacting their C&C servers. Sometimes, both malware have used the same C&C server, but in other cases, even the servers have been different.

Further reading

1. *Timo Hirvonen; F-Secure Labs; CosmicDuke: Cosmu with a Twist of MiniDuke; published 2 July 2014;* https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf
2. GReAT; Securelist; *Miniduke is back: Nemesis Gemina and the Botgen Studio;* published 3 July 2014; https://securelist.com/blog/incidents/64107/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/

MINIDUKE

First known activity:	◆ Loader July 2010 ◆ Backdoor May 2011
Most recent known activity:	◆ Loader Spring 2015 ◆ Backdoor Summer 2014
Other names:	N/A
C&C communication methods:	HTTP (S), Twitter
Known toolset components:	◊ Downloader ◊ Backdoor ◊ Loader

The MiniDuke toolset consists of multiple downloader and backdoor components, which are commonly referred to as the MiniDuke "stage 1", "stage 2", and "stage 3" components as per Kaspersky's original MiniDuke whitepaper. Additionally, a specific loader is often associated with the MiniDuke toolset and is referred to as the "MiniDuke loader".

While the loader has often been used together with other MiniDuke components, it has also commonly been used in conjunction with CosmicDuke and PinchDuke. In fact, the oldest samples of the loader that we have found were used with PinchDuke. To avoid confusion however, we have decided to continue referring to the loader as the "MiniDuke loader".

Two details about MiniDuke components are worth noting. Firstly, some of the MiniDuke components were written in Assembly language. While many malware were written in Assembly during the 'old days' of curiosity-driven virus writing, it has since become a rarity. Secondly, some of the MiniDuke components do not contain a hardcoded C&C server address, but instead obtain the address of a current C&C server via Twitter. The use of Twitter either to initially obtain the address of a C&C server (or as a backup if no hardcoded primary C&C server responds) is a feature also found in OnionDuke, CozyDuke, and HammerDuke.

Further reading

1. Costin Raiu, Igor Soumenkov, Kurt Baumgartner, Vitaly Kamluk; Kaspersky Lab; *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor;* published 27 February 2013; http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf
2. CrySyS Blog; *Miniduke;* published 27 February 2013; http://blog.crysys.hu/2013/02/miniduke/
3. Marius Tivadar, Bíró Balázs, Cristian Istrate; BitDefender; *A Closer Look at MiniDuke;* published April 2013; http://labs.bitdefender.com/wp-content/uploads/downloads/2013/04/MiniDuke_Paper_Final.pdf
4. CIRCL - Computer Incident Response Center Luxembourg; *Analysis Report (TLP:WHITE) Analysis of a stage 3 Miniduke sample;* published 30 May 2013; https://www.circl.lu/files/tr-14/circl-analysisreport-miniduke-stage3-public.pdf
5. ESET WeLiveSecurity blog; *Miniduke still duking it out;* published 20 May 2014; http://www.welivesecurity.com/2014/05/20/miniduke-still-duking/

COZYDUKE

First known activity:	January 2010
Most recent known activity:	Spring 2015
Other names:	CozyBear, CozyCar, Cozer, EuroAPT
C&C communication methods:	HTTP (S), Twitter (backup)
Known toolset components:	◊ Dropper ◊ Modular backdoor ◊ Multiple persistence components ◊ information gathering module ◊ Screenshot module ◊ Password stealing module ◊ Password hash stealing module

CozyDuke is not simply a malware toolset; rather, it is a modular malware platform formed around a core backdoor component. This component can be instructed by the C&C server to download and execute arbitrary modules, and it is these modules that provide CozyDuke with its vast array of functionality. Known CozyDuke modules include:

- Command execution module for executing arbitrary Windows Command Prompt commands
- Password stealer module
- NT LAN Manager (NTLM) hash stealer module
- System information gathering module
- Screenshot module

In addition to modules, CozyDuke can also be instructed to download and execute other, independent executables. In some observed cases, these executables were self-extracting archive files containing common hacking tools, such as PSExec and Mimikatz, combined with script files that execute these tools. In other cases, CozyDuke has been observed downloading and executing tools from other toolsets used by the Dukes such as OnionDuke, SeaDuke, and HammerDuke.

Further reading

1. Artturi Lehtio; F-Secure Labs; *CozyDuke;* published 22 April 2015; https://www.f-secure.com/documents/996508/ 1030745/CozyDuke

2. Kurt Baumgartner, Costin Raiu; Securelist; *The CozyDuke APT;* 21 April 2015; https://securelist.com/blog/research/69731/the-cozyduke-apt/

EXAMPLES OF COZYDUKE PDB STRINGS

- `E:\Visual Studio 2010\Projects\Agent_NextGen\Agent2011v3\Agent2011\Agent\tasks\bin\GetPasswords\exe\GetPasswords.pdb`
- `D:\Projects\Agent2011\Agent2011\Agent\tasks\bin\systeminfo\exe\systeminfo.pdb`
- `\\192.168.56.101\true\soft\Agent\tasks\Screenshots\agent_screeshots\Release\agent_screeshots.pdb`

ONIONDUKE

First known activity:	February 2013
Most recent known activity:	Spring 2015
Other names:	N/A
C&C communication methods:	HTTP (S), Twitter (backup)
Known toolset components:	◊ Dropper ◊ Loader ◊ Multiple modular core components ◊ information stealer ◊ Distributed Denial of Service (DDoS) module ◊ Password stealing module ◊ information gathering module ◊ Social network spamming module

The OnionDuke toolset includes at least a dropper, a loader, an information stealer trojan and multiple modular variants with associated modules.

OnionDuke first caught our attention because it was being spread via a malicious Tor exit node. The Tor node would intercept any unencrypted executable files being downloaded and modify those executables by adding a malicious wrapper contained an embedded OnionDuke. Once the victim finished downloading the file and executed it, the wrapper would infect the victim's computer with OnionDuke before executing the original legitimate executable.

The same wrapper has also been used to wrap legitimate executable files, which were then made available for users to download from torrent sites. Again, if a victim downloaded a torrent containing a wrapped executable, they would get infected with OnionDuke.

Finally, we have also observed victims being infected with OnionDuke after they were already infected with CozyDuke. In these cases, CozyDuke wasn instructed by its C&C server to download and execute OnionDuke toolset.

Further reading

1. Artturi Lehtio; F-Secure Weblog; *OnionDuke: APT Attacks Via the Tor Network;* published 14 November 2014; https://www.f-secure.com/weblog/archives/00002764.html

SEADUKE

First known activity:	October 2014
Most recent known activity:	Spring 2015
Other names:	SeaDaddy, SeaDask
C&C communication methods:	HTTP (S)
Known toolset components:	◊ Backdoor

SeaDuke is a simple backdoor that focuses on executing commands retrieved from its C&C server, such as uploading and downloading files, executing system commands and evaluating additional Python code. SeaDuke is made interesting by the fact that it is written in Python and designed to be cross-platform so that it works on both Windows and Linux.

The only known infection vector for SeaDuke is via an existing CozyDuke infection, wherein CozyDuke downloads and executes the SeaDuke toolset.

Like HammerDuke, SeaDuke appears to be used by the Dukes group primarily as a secondary backdoor left on CozyDuke victims after that toolset has completed the initial infection and stolen any readily available information from them.

Further reading

1. Symantec Security Response; *"Forkmeiamfamous": Seaduke, latest weapon in the Duke armory;* published 13 July 2015; http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory
2. Josh Grunzweig; Palo Alto Networks; *Unit 42 Technical Analysis: Seaduke;* published 14 July 2015; http://researchcenter.paloaltonetworks.com/2015/07/unit-42-technical-analysis-seaduke/
3. Artturi Lehtio; F-Secure Weblog; *Duke APT group's latest tools: cloud services and Linux support*; published 22 July 2015; https://www.f-secure.com/weblog/archives/00002822.html

EXAMPLE OF CROSS-PLATFORM SUPPORT FOUND IN SEADUKE'S SOURCE CODE

```
@property
def autoload_settings(self):
 windows_autoload_settings={'exe_name':'iexplore.exe','app_name':'Internet Explorer','self_delete':False}
 linux_autoload_settings={'exe_name':'httpd','app_name':'Apache','self_delete':False}
 if sys_platform=='win32':
  default_autoload_settings=windows_autoload_settings
 else:
  default_autoload_settings=linux_autoload_settings
 return v_conf_json.get('autoload_settings',default_autoload_settings)
```

HAMMERDUKE

First known activity:	January 2015
Most recent known activity:	Summer 2015
Other names:	HAMMERTOSS, Netduke
C&C communication methods:	HTTP (S), Twitter
Known toolset components:	◊ Backdoor

HammerDuke is a simple backdoor that is apparently designed for similar use cases as SeaDuke. Specifically, the only known infection vector for HammerDuke is to be downloaded and executed by CozyDuke onto a victim that has already been compromised by that toolset. This, together with HammerDuke's simplistic backdoor functionality, suggests that it is primarily used by the Dukes group as a secondary backdoor left on CozyDuke victims after CozyDuke performed the initial infection and steal any readily available information from them.

HammerDuke is however interesting because it is written in .NET, and even more so because of its occasional use of Twitter as a C&C communication channel. Some HammerDuke variants only contain a hardcoded C&C server address from which they will retrieve commands, but other HammerDuke variants will first use a custom algorithm to generate a Twitter account name based on the current date. If the account exists, HammerDuke will then search for tweets from that account with links to image files that contain embedded commands for the toolset to execute.

HammerDuke's use of Twitter and crafted image files is reminiscent of other Duke toolsets. Both OnionDuke and MiniDuke also use date-based algorithms to generate Twitter account names and then searched for any tweets from those accounts that linked to image files. In contrast however, for OnionDuke and MiniDuke the linked image files contain embedded malware to be downloaded and executed, rather than instructions.

Similarly, GeminiDuke may also download image files, but these would contain embedded additional configuration information for the toolset itself. Unlike Hammersmith however, the URLs for the images downloaded by GeminiDuke are hardcoded in its initial configuration, rather than retreived from Twitter.

Further reading

1. FireEye; HAMMERTOSS: *Stealthy Tactics Define a Russian Cyber Threat Group;* published July 2015; https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf *

*__APT29__ is the name used by FireEye to identify the cyberespionagegroup we refer to as the Dukes.

CLOUDDUKE

First known activity:	June 2015
Most recent known activity:	Summer 2015
Other names:	MiniDionis, CloudLook
C&C communication methods:	HTTP (S), Microsoft OneDrive
Known toolset components:	◊ Downloader ◊ Loader ◊ Two backdoor variants

CloudDuke is a malware toolset known to consist of, at least, a downloader, a loader and two backdoor variants. The CloudDuke downloader will download and execute additional malware from a preconfigured location. Interestingly, that location may be either a web address or a Microsoft OneDrive account.

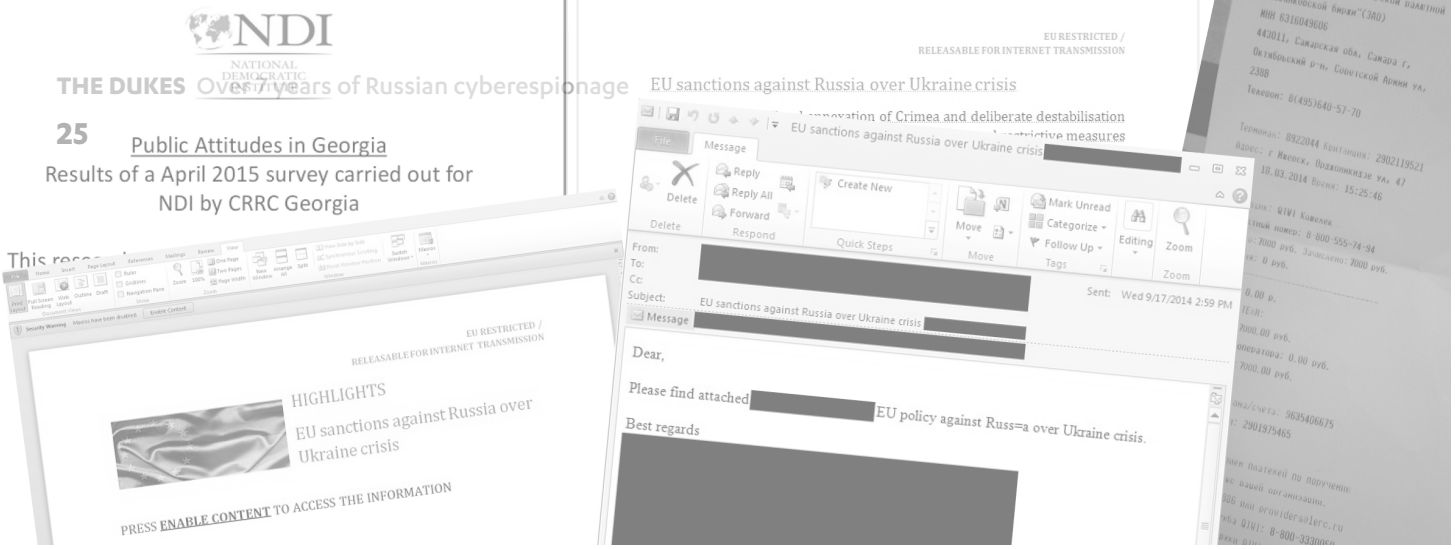
Both CloudDuke backdoor variants support simple backdoor functionality, similar to SeaDuke. While one variant will use a preconfigured C&C server over HTTP or HTTPS, the other variant will use a Microsoft OneDrive account to exchange commands and stolen data with its operators.

Further reading

1. Artturi Lehtio; F-Secure Weblog; *Duke APT group's latest tools: cloud services and Linux support*; published 22 July 2015; https://www.f-secure.com/weblog/archives/00002822.html

2. Brandon Levene, Robert Falcone and Richard Wartell; Palo Alto Networks; *Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke;* published 14 July 2015; http://researchcenter.paloaltonetworks.com/2015/07/tracking-minidionis-cozycars-new-ride-is-related-to-seaduke/

3. Segey Lozhkin; Securelist; *Minidionis – one more APT with a usage of cloud drives*; published 16 July 2015; https://securelist.com/blog/research/71443/minidionis-one-more-apt-with-a-usage-of-cloud-drives/



INFECTION VECTORS

The Dukes primarily use spear-phishing emails when attempting to infect victims with their malware. These spear-phishing emails range from ones purposely designed to look like spam messages used to spread common crimeware and addressed to large numbers of people, to highly targeted emails addressed to only a few recipients (or even just one person) and with content that is highly relevant for the intended recipient(s). In some cases, the Dukes appear to have used previously compromised victims to send new spear-phishing emails to other targets.

The spear-phishing emails used by the Dukes may contain either specially-crafted malicious attachments or links to URLs hosting the malware. When malicious attachments are used, they may either be designed to exploit a vulnerability in a popular software assumed to be installed on the victim's machine, such as Microsoft Word or Adobe Reader, or the attachment itself may have its icon and filename obfuscated in such a way that the file does not appear to be an executable.

The only instances which we are aware of where the Dukes did not use spear-phishing as the initial infection vector is with certain **OnionDuke** variants. These were instead spread using either a malicious Tor node that would trojanize legitimate applications on-the-fly with the **OnionDuke** toolset, or via torrent files containing previously trojanized versions of legitimate applications.

Finally, it is worth noting that the Dukes are known to sometimes re-infect a victim of one of their malware tools with another one of their tools. Examples include **CozyDuke** infecting its victims with **SeaDuke** or **HammerDuke**, and **OnionDuke** and **CosmicDuke** infecting its victims with **PinchDuke** or **GeminiDuke**.

DECOYS

The Dukes commonly employ decoys with all of their infection vectors. These decoys may be image files, document files, Adobe Flash videos or similar that are presented to the victim during the infection process in an attempt to distract them from the malicious activity. The contents of these decoys range from non-targeted material such as videos of television commercials purporting showing monkeys at an office, to highly targeted documents with content directly relevant to the intended recipient such as reports, invitations, or lists of participants to an event.

Usually, the contents of the decoys appear to be taken from public sources, either by copying publicly accessible material such as a news report or by simply repurposing a legitimate file that has been openly distributed. In some cases however, highly targeted decoys have been observed using content that does not appear to be publicly available, suggesting that these contents may have been stolen from other victims that had been infected by Duke toolsets.

EXPLOITATION OF VULNERABILITIES

The Dukes have employed exploits both in their infection vectors as well as in their malware. We are however only aware of one instance - the exploitation of CVE-2013-0640 to deploy **MiniDuke** - where we believe the exploited vulnerability was a zero-day at the time that the group acquired the exploit. In all known cases where exploits were employed, we believe the Dukes did not themselves discover the vulnerabilities or design the original exploits; for the exploited zero-day, we believe the Dukes purchased the exploit. In all other cases, we believe the group simply repurposed publicly available exploits or proofs of concept.

Map of timezones in Russia; © Eric Muller
Pink: MSK (UTC +3) ; Orange: UTC +4

ATTRIBUTION AND STATE-SPONSORSHIP

Attribution is always a difficult question, but attempting to answer it is important in understanding these types of threats and how to defend against them. This paper has already stated that we believe the Dukes to be a Russian state-sponsored cyberespionage operation. To reach this conclusion, we began by analyzing the apparent objectives and motivations of the group.

Based on what we currently know about the targets chosen by the Dukes over the past 7 years, they appear to have consistently targeted entities that are deal with foreign policy and security policy matters. Organizations that include ministries of foreign affairs, embassies, senates, parliaments, ministries of defense, defense contractors, and think tanks all appear to have been the primary targets of the group.

In one of their more intriguing cases, the Dukes have appeared to also target entities involved in the trafficking of illegal drugs. Even such targets however appear to be consistent with the overarching theme, given the drug trade's relevance to security policy. Based on this, we are confident in our conclusion that the Dukes' primary mission is the collection of intelligence to support foreign and security policy decision-making.

This naturally leads to the question of state-sponsorship. Based on our establishment of the group's primary mission, we believe the main benefactor (or benefactors) of their work is a government. But are the Dukes a team or a department inside a government agency? an external contractor? A criminal gang selling to the highest bidder? A group of tech-savvy patriots? We don't know.

Based on the length of the Dukes' activity, our estimate of the amount of resources invested in the operation and the fact that their activity only appears to be increasing, we believe the group to have significant and most critically, stable financial backing. The Dukes have consistently operated large-scale campaigns against high-profile targets while concurrently engaging in smaller, more targeted campaigns with apparent coordination and no evidence of unintentional overlap or operational clashes. We therefore believe the Dukes to be a single, large, well-coordinated organization with clear separation of responsibilities and targets.

The Dukes appear to prioritize the continuation of their operations over stealth. Their 2015 **CozyDuke** and **CloudDuke** campaigns take this to the extreme by apparently opting for speed and quantity over stealth and quality. In the most extreme case, the Dukes continued with their July 2015 **CloudDuke** campaign even after their activity had been outed by multiple security vendors. We therefore believe the Dukes' primary mission to be so valuable to their benefactors that its continuation outweighs everything else.

This apparent disregard for publicity suggests, in our opinion, that the benefactors of the Dukes is so powerful and so tightly connected to the group that they are able to operate with no apparent fear of repercussions on getting caught. We believe the only benefactor with the power to offer such comprehensive protection would be the government of the nation from which the group operates. We therefore believe the Dukes to work either within or directly for a government, thus ruling out the possibility of a criminal gang or another third party.

This leaves us with the final question: which country? We are unable to conclusively prove responsibility of any specific country for the Dukes. All of the available evidence however does in our opinion suggest that the group operates on behalf of the Russian Federation. Further, we are currently unaware of any evidence disproving this theory.

Kaspersky Labs has previously noted the presence of Russian-language artefacts in some of the Duke malware samples [10]. We have also found a Russian-language error message in many **PinchDuke** samples: "Ошибка названия модуля! Название секции данных должно быть 4 байта!" This roughly translates as, "There is an error in the module's name! The length of the data section name must be 4 bytes!"

Additionally, Kaspersky noted that based on the compilation timestamps, the authors of the Duke malware appear to primarily work from Monday to Friday between the times of 6am and 4pm UTC+0 [12]. This corresponds to working hours between 9am and 7pm in the UTC+3 time zone, also known as Moscow Standard Time, which covers, among others, much of western Russia, including Moscow and St. Petersburg.

The Kaspersky Labs analysis of the Duke malware authors' working times is supported by our own analysis, as well as that performed by FireEye [23]. This assertion of time zone is also supported by timestamps found in many **GeminiDuke** samples, which similarly suggest the group work in the Moscow Standard Time timezone, as further detailed in the section on the technical analysis of **GeminiDuke** (page 17).

Finally, the known targets of the Dukes - Caucasian foreign ministries, western think tanks and governmental organizations, even Russian-speaking drug dealers - conform to publicly-known Russian foreign policy and security policy interests. Even though the Dukes appear to have targeted governments all over the world, we are unaware of them ever targeting the Russian government. While absence of evidence is not evidence of absence, it is an interesting detail to note.

Based on the presented evidence and analysis, we believe, with a high level of confidence, that the Duke toolsets are the product of a single, large, well-resourced organization (which we identify as the Dukes) that provides the Russian government with intelligence on foreign and security policy matters in exchange for support and protection.

BIBLIOGRAPHY

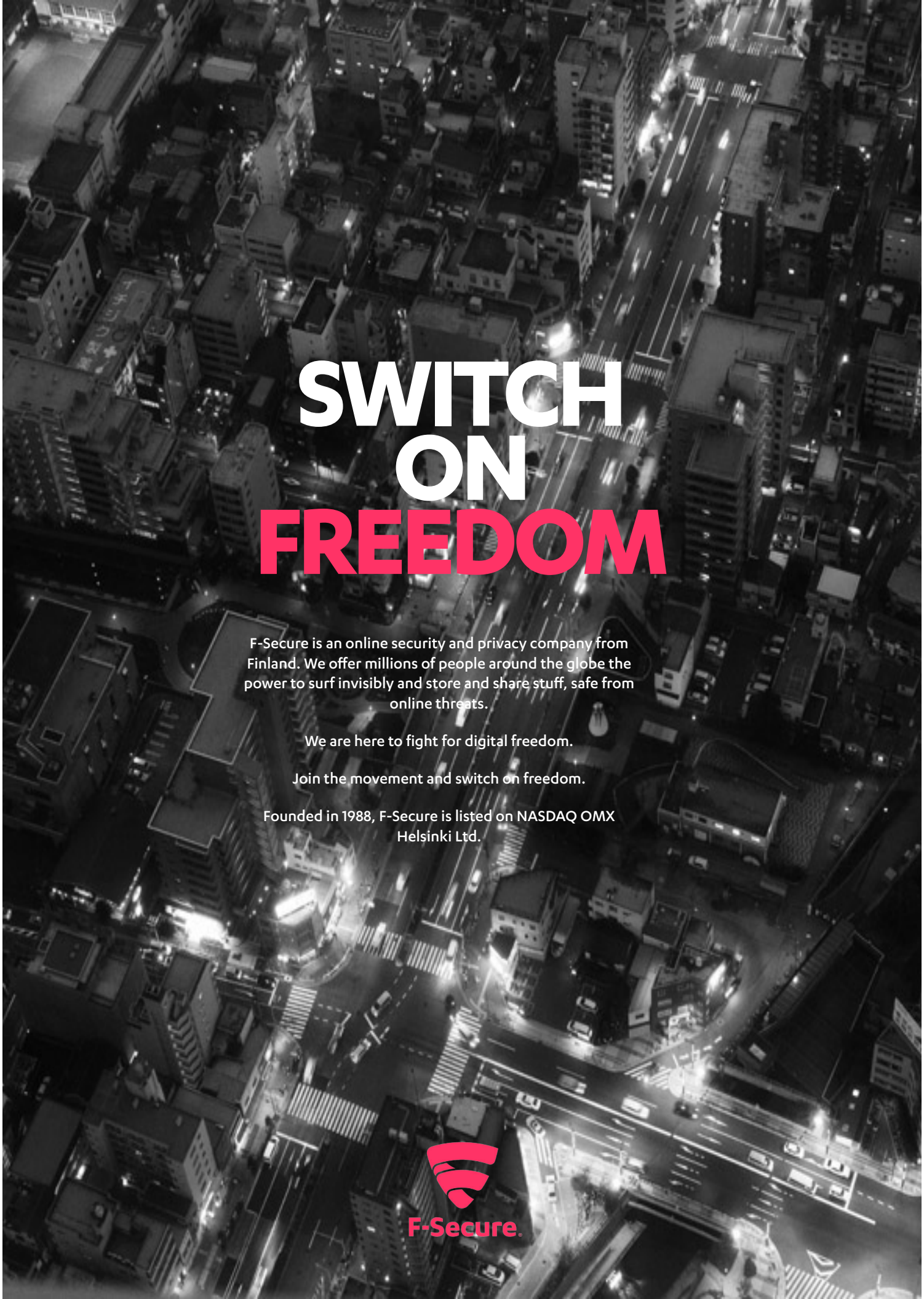
1. The White House; *Remarks By President Barack Obama In Prague As Delivered;* published 5 April 2009; [Online]. Available: https://www.whitehouse.gov/the-press-office/remarks-president-barack-obama-prague-delivered
2. Peter Baker; New York Times; *White House Scraps Bush's Approach to Missile Shield;* published 17 September 2009; [Online]. Available: http://www.nytimes.com/2009/09/18/world/europe/18shield.html
3. Wikipedia; *KavKaz Center;* [Online]. Available: https://en.wikipedia.org/wiki/Kavkaz_Center
4. BBC: *Nato exercises 'a dangerous move';* published 17 April 2009; [Online]. Available:http://news.bbc.co.uk/2/hi/europe/8004399.stm
5. Tavis Ormandy; Seclists.org; Microsoft Windows NT #GP Trap Handler Allows Users to Switch Kernel Stack; published 19 January 2010; [Online]. Available: http://seclists.org/fulldisclosure/2010/Jan/341
6. Timo Hirvonen; F-Secure Labs; *CosmicDuke: Cosmu with a Twist of MiniDuke;* published 2 July 2014; [Online]. Available: https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf
7. Yichong Lin, James T. Bennett, Thoufique Haq; FireEye Threat Research blog; *In Turn, It's PDF Time;* published 12 February 2013; [Online]. Available: https://www.fireeye.com/blog/threat-research/2013/02/in-turn-its-pdf-time.html
8. Costin Raiu, Igor Soumenkov, Kurt Baumgartner, Vitaly Kamluk; *Kaspersky Lab; The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor;* published 27 February 2013; [Online]. Available: http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf
9. Laboratory of Cryptography and System Security (CrySyS Lab); Miniduke: Indicators; published 27 February 2013; [Online]. Available: http://www.crysys.hu/miniduke/miniduke_indicators_public.pdf
10. Mikko Hypponen; F-Secure Weblog; Targeted Attacks and Ukraine; published 1 April 2014; [Online]. Available: https://www.f-secure.com/weblog/archives/00002688.html
11. Feike Hacquebord; Trend Micro; *Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets;* published 18 August 2015; [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/
12. GReAT; Securelist; *Miniduke is back: Nemesis Gemina and the Botgen Studio;* published 3 July 2014; [Online]. Available: https://securelist.com/blog/incidents/64107/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/
13. Boost C++ Libraries; *Version 1.54.0;* published 1 July 2013; [Online]. Available: http://www.boost.org/users/history/version_1_54_0.html
14. Artturi Lehtio; F-Secure Weblog; *OnionDuke: APT Attacks Via the Tor Network;* published 14 November 2014; [Online]. Available: https://www.f-secure.com/weblog/archives/00002764.html
15. Artturi Lehtio; F-Secure Labs; *CozyDuke;* published 22 April 2015; [Online]. Available: https://www.f-secure.com/documents/996508/ 1030745/CozyDuke
16. Symantec Security Response; *"Forkmeiamfamous": Seaduke, latest weapon in the Duke armory;* published 13 July 2015; [Online]. Available: http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory
17. Brandon Levene, Robert Falcone and Richard Wartell; Palo Alto Networks; *Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke;* published 14 July 2015; [Online]. Available: http://researchcenter.paloaltonetworks.com/2015/07/tracking-minidionis-cozycars-new-ride-is-related-to-seaduke/
18. Segey Lozhkin; Securelist; *Minidionis – one more APT with a usage of cloud drives*; published 16 July 2015; [Online]. Available: https://securelist.com/blog/research/71443/minidionis-one-more-apt-with-a-usage-of-cloud-drives/
19. malware@prevenity; *Malware w 5 rocznicę katastrofy samolotu;* published 22 April 2015; [Online]. Available: http://malware.prevenity.com/2015/04/malware-w-5-rocznice-katastrofy-samolotu.html
20. malware@prevenity; *Wykradanie danych z instytucji publicznych;* published 11 August 2015; [Online]. Available: http://malware.prevenity.com/2015/08/wykradanie-danych-z-instytucji.html
21. Wikipedia; *Moscow Time;* [Online]. Available: https://en.wikipedia.org/wiki/Moscow_Time
22. Exploit Database; CVE: 2010-4398; published 24 November 2014; [Online]. Available: https://www.exploit-db.com/exploits/15609/
23. FireEye; HAMMERTOSS: *Stealthy Tactics Define a Russian Cyber Threat Group;* published July 2015; [Online]. Available: https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf *
24. tz_world, an efele.net/tz map; Eric Muller*; tz_russia, an efele.net/tz map: A shapefile of the TZ timezones of Russia*; published 2 May 2013; [Online]. Available: http://efele.net/maps/tz/russia/

APPENDIX I: DATA LISTINGS

PinchDuke

Campaign identifiers

- alkavkaz.com20081105
- cihaderi.net20081112
- 20090111
- diploturk_20090305_faruk
- 20090310l
- mofa.go.ug_20090317
- plcz_20090417
- 20090421_NN1
- 20090427_n_8
- 20090513_Cr
- natoinfo_ge
- 20090608_G
- mod_ge_2009_07_03
- 20090909_Bel
- mofa-go-ug-2009-09-09
- 20091008_Af
- nat_20092311
- turtsia_20091128
- mfagovtr_20091204
- modge_20100126
- GEN20100215
- par_ge_20100225
- pr_ge_20100225
- tika_20100326
- harpa_20100329
- sanat_20100412
- mfakg_20100413
- leskz_20100414
- leskg_20100422
- az_emb_uz_20100518
- sat_20100524
- emb_azerb_uz_20100609
- sat_2010_07_26
- kaz_2010_07_30


SWITCH
ON
FREEDOM
F-Secure is an online security and privacy company from Finland. We offer millions of people around the globe the power to surf invisibly and store and share stuff, safe from online threats.
We are here to fight for digital freedom.
Join the movement and switch on freedom.
Founded in 1988, F-Secure is listed on NASDAQ OMX Helsinki Ltd.
F-Secure.