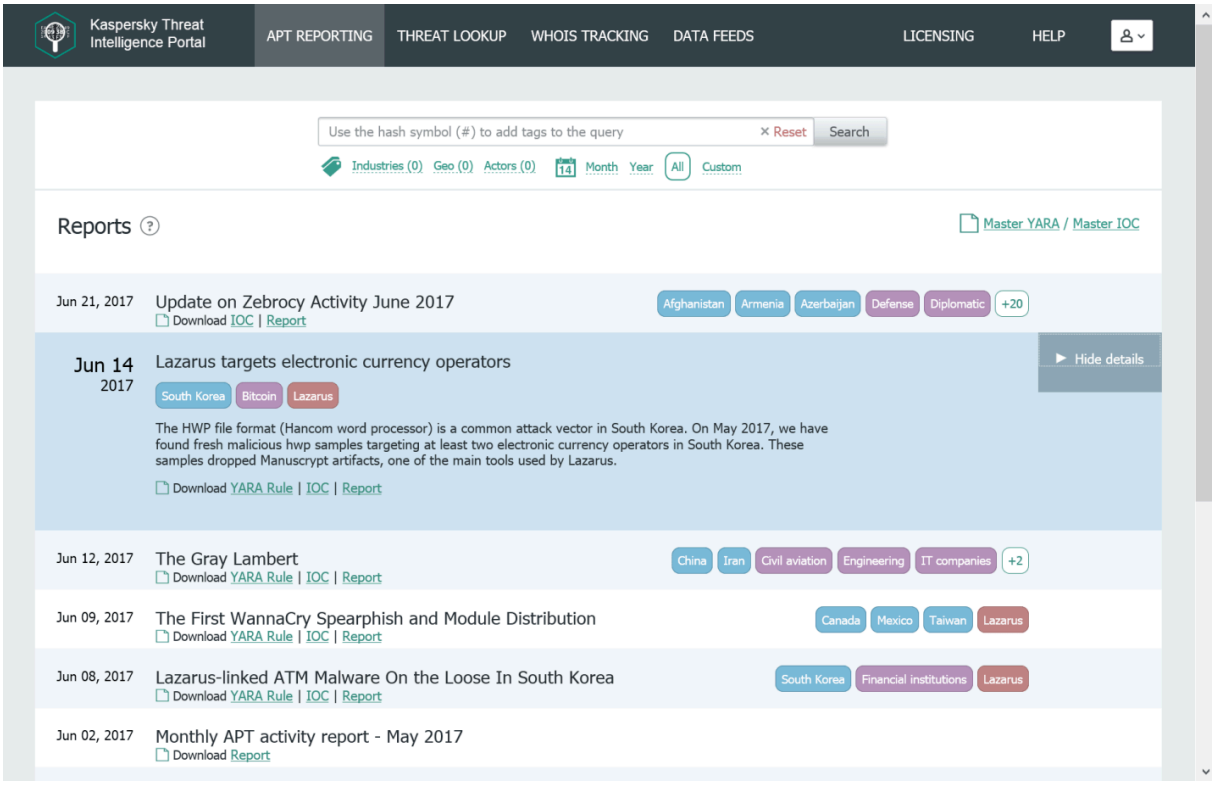
APT Trends report Q2 2017

By GReAT

Published: 2017-08-08 · Archived: 2026-04-05 17:24:20 UTC

Introduction

Since 2014, Kaspersky Lab's Global Research and Analysis Team (GReAT) has been providing threat intelligence reports to a wide-range of customers worldwide, leading to the delivery of a full and dedicated private reporting service. Prior to the new service offering, GReAT published research online for the general public in an effort to help combat the ever-increasing threat from nation-state and other advanced actors. Since we began offering a threat intelligence service, all deep technical details on advanced campaigns are first pushed to our subscriber base. At the same time, to remain true to our efforts to help make the internet safer, important incidents, such as WannaCry or Petya are covered in both private and public reports.



Kaspersky's Private Threat Intelligence Portal (TIP)

In Q1 of 2017 we published our first APT Trends report, highlighting our top research findings over the last few months. We will continue to publish quarterly reports as a representative snapshot of what has been offered in greater detail in our private reports in order to highlight significant events and findings we feel most users should be aware of. If you would like to learn more about our intelligence reports or request more information for a specific report, readers are encouraged to contact: **intelreports@kaspersky.com**.

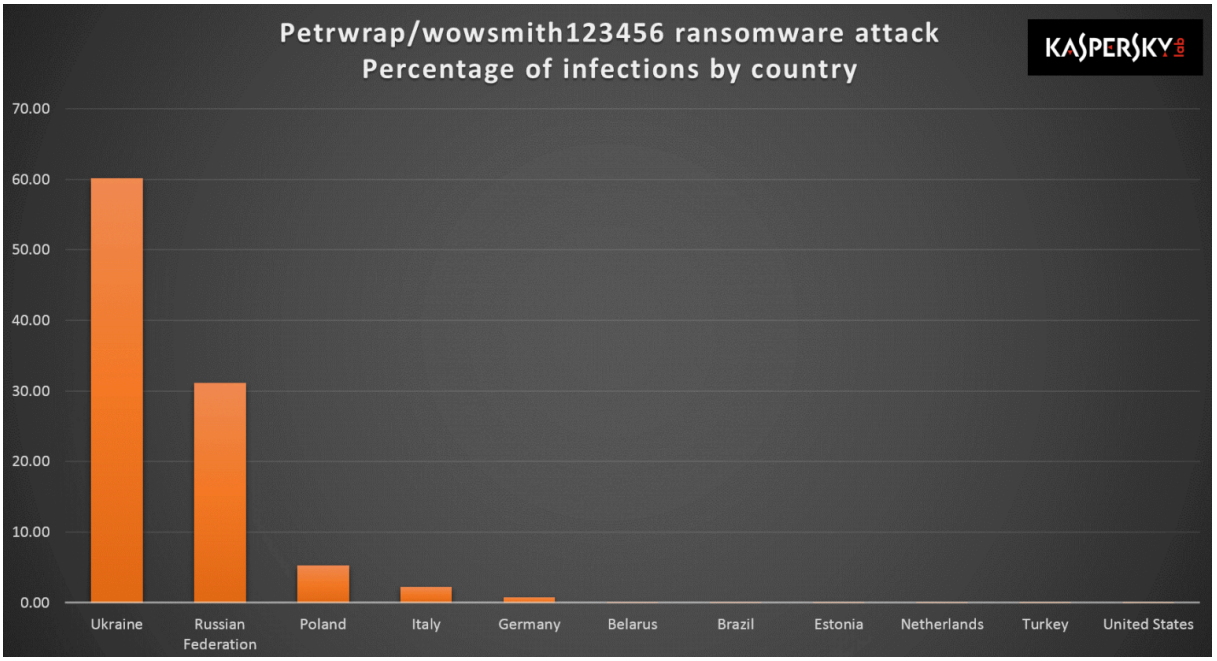
Russian-Speaking Actors

The second quarter of 2017 has seen multiple incidents involving Russian-speaking threat actors. Topping the list of ‘attention grabbers’ were the Sofacy and Turla threat actors.

March and April started off with a bang, with the discovery of three zero-day exploits being used in-the-wild by Sofacy and Turla: two of these targeted Microsoft Office’s Encapsulated PostScript (EPS) and the third being a Microsoft Windows Local Privilege Escalation (LPE). Sofacy was discovered utilizing both CVE-2017-0262 (an EPS vulnerability) and CVE-2017-0263 (LPE) over the Easter holiday, targeting a swath of users throughout Europe. Prior to this attack, Turla was also discovered using CVE-2017-0261 (a different EPS vulnerability). Neither actor appeared to deviate from their usual payload repertoire, with Sofacy dropping their typical GAMEFISH payload and Turla utilizing what we refer to as ICEDCOFFEE (a.k.a. Shirime). Targeting for these attacks was also directly within the normal wheelhouse for both actors, focusing mainly on foreign ministries, governments, and other government-affiliated organizations.

GReAT produced additional reports on Sofacy and Turla beyond those mentioned above. In April, we notified customers of two new experimental macro techniques utilized by Sofacy. These techniques, while not particularly sophisticated, caught our attention as they had not been seen before in-the-wild. The first technique involved using the built-in ‘certutil’ utility in Microsoft Windows to extract a hardcoded payload within a macro. The second technique involved embedding Base64-encoded payloads within the EXIF metadata of the malicious documents. While the targeting for this new set of activity was again fairly standard, we discovered some noteworthy targeting against a French political party member prior to the 2017 elections. Moving into May and June, we wrote two additional reports of interest involving these two actors: the first was an update on the long running “Mosquito Turla” campaign showing the usage of fake Adobe Flash installers and continued targeting of foreign Ministries. The other documented yet another update on Sofacy’s unique Delphi payload we call ‘Zebrocy’.

June saw the massive outbreak of a piece of malware dubbed “ExPetr”. While initial assessments presumed that this was yet another ransomware attack a la WannaCry, a deeper assessment by GReAT places the initial intent as constituting an operation destructive in nature. We were also able to confidently identify the initial distribution of the malware, as well as indicate a *low confidence* assessment that the attacks may share traits with the BlackEnergy actors.



Below is a summary of report titles produced for the Eastern European region only. As stated above, if you would like to learn more about our threat intelligence products or request more information on a specific report, please direct inquiries to **intelreports@kaspersky.com**.

1. 1 Sofacy Dabbling in New Macro Techniques
2. 2 Sofacy Using Two Zero Days in Recent Targeted Attacks – early warning
3. 3 Turla EPS Zero Day – early warning
4. 4 Mosquito Turla Targets Foreign Affairs Globally
5. 5 Update on Zebrocy Activity June 2017
6. 6 ExPetr motivation and attribution – Early alert
7. 7 BlackBox ATM attacks using SDC bus injection

English-Speaking Actors

English-speaking actors are always particularly fascinating due to their history of complex tooling and campaigns. Actors like Regin and Project Sauron have proven fascinating examples of new techniques leveraged in long-lasting, hard to catch campaigns and as such make ideal subjects for further research. Not to be outdone, Equation and the Lamberts were the subjects of our most recent investigations.

Continuing our practice of conducting malware paleontology while integrating new discoveries, we published a report on EQUATIONVECTOR, an Equation backdoor first used as early as 2006. This backdoor is a fascinating passive-active shellcode staging implant. It's one of the earliest noted instances of a NObody But US ('NOBUS') backdoor for staging further attacks. Despite its age, the EQUATIONVECTOR backdoor (identified as 'PeddleCheap' in the latest ShadowBrokers disclosures) incorporates many advanced techniques for prolonged stealthy operations in victim networks, allowing the Equation operators to deliver further payloads without arousing suspicion. The report tracks the development of these tools through subsequent iterations year-by-year.

Our tracking of the Lamberts toolkit continues with the publication of the Gray Lambert report in June, the most advanced Lambert known to date. This too is a NOBUS backdoor, a passive implant operating strictly in user-land. The intricate usefulness of Gray Lambert lies in its ability to orchestrate multiple sniffer victims on a network via broadcast, multicast, and unicast commands, allowing the operators to employ surgical precision in networks with many infected machines. The sniffers double as next-stage payload delivery mechanisms for an infected network. A notable feature of the Lambert campaigns is the level of precision with which targets are chosen; Gray Lambert's victimology is primarily focused on strategic verticals in Asia and Middle East. During this investigation, GReAT researchers have also discovered two additional Lambert families (Red Lambert and Brown Lambert) currently under investigation for Q3. Below is a list of report titles for reference:

1. 1 EQUATIONVECTOR – A Generational Breakdown of the PeddleCheap Multifunctional Backdoor
2. 2 The Gray Lambert – A Leap in Sophistication to User-land NOBUS Passive Implants

Korean-speaking Actors

Our researchers focusing on attacks with a Korean nexus also had a very busy quarter, producing seven reports on the Lazarus group and WannaCry attacks. Most of the reports on Lazarus directly involved a sub-group we refer to as BlueNoroff. They are the arm that focuses mainly on financial gain, targeting banks, ATMs, and other "money-makers". We revealed to customers a previously unknown piece of malware dubbed 'Manuscrypt' used by Lazarus to target not only diplomatic targets in South Korea, but also people using virtual currency and electronic payment sites. Most recently, 'Manuscrypt' has become the primary backdoor used by the BlueNoroff sub-group to target financial institutions.

WannaCry also created quite a stir in the second quarter, with our analysts producing three reports and multiple blog posts on this emerging threat. What proved most interesting to us, was the probable linkage to Lazarus group as the source of the attacks, as well as the origins of the malware. GReAT researchers were able to trace back some of its earliest usage and show that before the 'EternalBlue' exploit was added to version 2, WannaCry v1 was used in spearphishing attacks months prior. Here is a listing of our reports from Q2 on actors with a Korean nexus:

1. 1 Manuscrypt – malware family distributed by Lazarus
2. 2 Lazarus actor targets carders
3. 3 Lazarus-linked ATM Malware On the Loose In South Korea
4. 4 Lazarus targets electronic currency operators
5. 5 WannaCry – major ransomware attack hitting businesses worldwide – early alert
6. 6 WannaCry possibly tied to the Lazarus APT Group
7. 7 The First WannaCry Spearphish and Module Distribution

Middle Eastern Actors

While there wasn't much high-end activity involving Middle Eastern actors, we did produce two reports revolving around the use of a zero-day exploit (CVE-2017-0199). The most notable involved an actor we refer to as BlackOasis and their usage of the exploit in-the-wild prior to its discovery. We have previously reported on BlackOasis using other zero-days in the past; CVE-2016-4117 in May 2016, CVE-2016-0984 in June 2015, and

CVE-2015-5119 in June 2015. It is believed that BlackOasis is a customer of Gamma Group and utilizes the popular ‘lawful surveillance’ kit FinSpy. Other than the usage of the exploit, this report was significant because it also showed one of the earliest known uses of a new version of FinSpy, which is still being analyzed by our researchers.

After the discovery of CVE-2017-0199, a plethora of threat actors also began to leverage this exploit in their attacks. We reported to customers on the usage of this exploit by a well-known Middle Eastern actor dubbed ‘OilRig’. OilRig has actively targeted many organizations in Israel with the exploit via spearphishes appearing to originate from well-known doctors within Ben Gurion University. While their execution was less than stellar, it highlighted the widespread usage of this exploit shortly after its discovery.

1. 1 OilRig exploiting CVE-2017-0199 in new campaign
2. 2 BlackOasis using Ole2Link zero day exploit in the wild

Chinese-Speaking Actors

On the Chinese speaking front, we felt it necessary to produce two reports to our customers. While Chinese speaking actors are active on a daily basis, not much has changed and we prefer to avoid producing reports on ‘yet another instance of APTxx’ for the sake of padding our numbers. Instead we try to focus on new and exciting campaigns that warrant special attention.

One of those reports detailed a new finding regarding a fileless version of the well-known ‘HiKit’ malware dubbed ‘Hias’. We have reported on Hias in the past, and one of our researchers was finally able to discover the persistence mechanism used, which also allowed us to tie the activity to an actor we call ‘CloudComputating’.

Another report detailed a new campaign we referred to as ‘IndigoZebra’. This campaign was targeting former Soviet Republics with a wide swath of malware including Meterpreter, Poison Ivy, xDown, and a previously unknown malware called ‘xCaon’. This campaign shares ties with other well-known Chinese-speaking actors, but no definitive attribution has been made at this time.

1. 1 Updated technical analysis of Hias RAT
2. 2 IndigoZebra – Intelligence preparation to high-level summits in Middle Asia

Best of the rest

Sometimes we find new and exciting campaigns or entirely new threat actors to report to our subscribers without being able to make an immediate or definitive determination on regional provenance. Several reports fell into this category in the last quarter. ChasingAdder is a report describing a new persistence technique that hijacked a legitimate WMI DLL for the purposes of loading a malicious payload. This activity targeted high-profile diplomatic, military, and research organizations beginning in the fall of 2016, but to date we have not been able to pinpoint the specific actor responsible.

Demsty is a new piece of MacOS malware that is targeting University researchers in Hong Kong, among others. At the time of writing, we have a low confidence assessment that the campaign was conducted by Chinese-speaking actors, and thus categorize this as ‘Unknown’ until greater evidence comes to light.

During Q2, the mischievous ShadowBrokers also continued their regular activities dumping multiple tools and documentation allegedly stolen from Equation Group. In April, the ShadowBrokers released another dump of information detailing the alleged targeting of SWIFT service bureaus and other banks by Equation Group. Since some of our customers are financial entities, we found it necessary to evaluate the data and provide an expert's opinion on the validity of the dump.

Reports in the 'unknown' category:

1. 1 ShadowBrokers' Lost in translation leak – SWIFT attacks analysis
2. 2 ChasingAdder – WMI DLL Hijacking Trojan Targeting High Profile Victims
3. 3 University Researchers Located in Hong Kong Targeted with Demsty

Predictions

Based on the trends we've seen over the last three months, as well as foreseeable geopolitical events, we have listed a few predictions for the upcoming quarter (Q3). As always, this isn't an exact science and some cases won't come to fruition. Analyzing current and future events and combining those with the motivations of known active actors can help organizations prepare for likely forthcoming activity:

1. 1 Misinformation campaigns will remain a threat to countries with upcoming elections, specifically Germany and Norway, as they have been previous targets for Eastern European based actors.
2. 2 'Lawful Surveillance' tools will continue to be utilized by governments that don't have well-established Cyber Operations capabilities, mainly based out of the Middle East. Companies such as Gamma Group, Hacking Team, and NSO will continue to offer new zero-day exploits to those customers. As prices increase and exchanges thrive, new organizations and marketplaces will continue popping up.
3. 3 Destructive malware disguised as ransomware will continue to be a problem. In the last quarter we've seen two instances of this, and with the continued release of tools / exploits from dumps like Vault7 and ShadowBrokers, this is going to be a new alarming trend to deal with.
4. 4 In China, the past months have been marked by the dwindling economic growth, rising tensions with North Korea and the US, and increased exchanges between South Korean / Japanese / American organizations. In addition to these, the 19th Party Congress is set to be held in the fall of 2017 and according to multiple public predictions, it is likely that some major changes will happen in the leadership. It's possible that these events will have wide regional influences that could affect the way that threat actors operate in Asia, both in terms of targeting and TTPs.
5. 5 Targeting energy-related companies and organizations will be on the rise. Countries such as Norway may be a top target moving forward given their control on oil and gas in the region in the buildup to an election. Saudi Arabia will also top the charts for potential targeting as they have in years past.
6. 6 Lower-tier threat actors continue to increase cyber-espionage efforts and capabilities both in complexity and size. Expect more activity with varied technical capabilities coming from lesser known or previously unseen actors.

How to keep yourself protected

One of the biggest problems when it comes to leveraging threat intelligence is judging the quality of the data and how it can be used for defense. For instance, we may observe an increase in the number of fileless attacks or attacks in which all IOCs are unique or specific per victim. In such situations, having not only host-based IOCs, but also network IOCs and Yara rules that can help identify malware in all cases is very important.

Another problem comes from the fact that many threat intelligence providers have a limited world view and their data covers only a small set of threats. It's easy for an enterprise to fall into the trap of thinking that 'actor X' is not something they need to worry because their focus has been only certain countries or certain industry sectors; only to discover later that their ignorance left them blind to those attacks.

As shown by many incidents, but especially by WannaCry and ExPetr's EternalBlue-based spreading subroutines, vulnerabilities remain a key approach to infecting systems. Therefore timely patching is of utmost importance – which, being one of the most tedious IT maintenance tasks, works much better with good automation. Kaspersky Endpoint Security for Business Advanced and Kaspersky Total Security include Vulnerability & Patch management components, offering convenient tools for making patching much easier, and much less time-consuming for IT staff.

Given the above, it is highly recommended that prevention (such as endpoint protection) along with advanced detection capabilities, such as a solution that can detect all types of anomalies and scrutinize suspicious files at a deeper level, be present on users' systems. The Kaspersky Anti Targeted Attack solution (KATA) matches events coming from different infrastructure levels, discerns anomalies and aggregates them into incidents, while also studying related artifacts in a safe environment of a sandbox. As with most Kaspersky products, KATA is powered by HuMachine Intelligence, which is backed by on premise and in lab-running machine learning processes coupled with real-time analyst expertise and our understanding of threat intelligence big data.

The best way to prevent attackers from finding and leveraging security holes, is to eliminate the holes altogether, including those involving improper system configurations or errors in proprietary applications. For this, Kaspersky Penetration Testing and Application Security Assessment services can become a convenient and highly effective solution, providing not only data on found vulnerabilities, but also advising on how to fix it, further strengthening corporate security.

https://www.youtube.com/watch?v=JS4tbSWQb90&width=640&height=360
