Case Study
APT28 Cybergroup Activity

Michal Ostrowski
michal.ostrowski@fireeye.com
Tomasz Pietrzyk
tomasz.pietrzyk@fireeye.com

SECURITY REIMAGINED

Instead of Marketing Slides… ☺

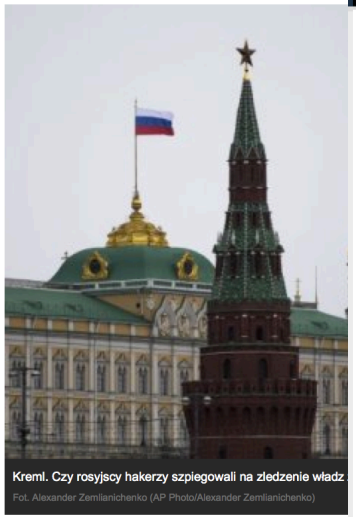
- FireEye/Mandiant monitors about 300 APT groups over the world continuously
  - They represent various TTPs (tools, techniques, and practices) and have various goals
  - They have something in common – they are highly skilled and extremely difficult to detect

Poland and Eastern Europe are not “no-APT-islands”…

Menu

Rosyjscy hakerzy zaatakowali jedną z p
Szpiegowali na zlecenie Moskwy?

osi, PAP 2014-10-14



Kreml. Czy rosyjscy hakerzy szpiegowali na zledzenie władz

Fot. Alexander Zemlianichenko (AP Photo/Alexander Zemlianichenko)

**Rosyjscy hakerzy, prawdopodobnie pracujący na z
nieznaną dotąd lukę w systemie operacyjnym Wind
instytucji, w tym polskiej firmy energetycznej - pod**

Amerykański dziennik powołuje się na raport firmy iSig
cybernetycznym. W dokumencie poinformowano, że gr
czasu szpiegowała m.in. instytucje NATO, ukraiński rza
zachodnioeuropejskiego rządu i francuską firmę teleko
z polskich firm z branży energetycznej; jej nazwa nie z

COMPUTERWORLD WIADOMOŚCI

TEMATY | Aplikacje Biznesowe | Bezpieczeństwo | Big Data

Grupa Dragonfly atakuje ró
firmy energetyczne

Najnowsza analiza firmy Symantec pokazuje, że grupa
prowadziła od 2013 roku ukierunkowane ataki na firmy
w Polsce.

Janusz Chustecki
01.07.2014, godz. 18:56

Share 1 | Tweet 1 | Lubię to! 3

Kilka dni temu pisaliśmy tutaj, że znany malware Stuxr
szkodliwe oprogramowanie noszące nazwę Havex. Ob
firma Symantec, publikując obszerny materiał opisując
grupa Dragonfly przeprowadziła ukierunkowane ataki s
energetycznego, w różnych krajach na świecie.

Wśród celów znaleźli się producenci energii, operatorz
specjalnych dla sektora energetycznego, zwłaszcza ze
Hiszpanii, ale także Niemiec, Francji, Szwajcarii, Wielk
Turcji, Kanadzie i Australii.

Operacja Ke3chang - chińscy hakerzy atakują europejską dyplomację

OPUBLIKOWANO: WTOREK, 17 GRUDNIA 2013, 18:30

Fot. polskiemedium.wordpress.com

D24 DEFENCE 24
kontakt@defence24.pl

4 | 4 | 2 | 0 | 5
Like | Share | Tweet | 8+1 | Share

DOTYCZY: CYBERBEZPIECZEŃSTWO, EUROPA

Wciąż nie ustają ataki chińskich hakerów wymierzone w europejskie ministerstwa spraw zagranicznych.

Jak podaje w swoim raporcie firma FireEye, specjalizująca się w dziedzinie zwalczania internetowych zagrożeń, Chiny przeprowadzają zaawansowane ataki hakerskie, które są bezpośrednio wymierzone w europejskie ministerstwa spraw zagranicznych. Chiński rząd odcina się tych działań, odrzuca oskarżenia pod swoim adresem zapewniając, że dąży do zwalczania cyberzagrożeń.

APT28 Key Findings

- APT28 targets insider information related to governments, militaries, and security organizations that would likely benefit the Russian government. APT28 primarily targets Georgia, Eastern Europe, and European security organizations using skillfully engineered malware which was created during normal working hours in Moscow.

APT28 TARGETING REFLECTS

RUSSIAN INTERESTS

APT28 Primary Targets

GEORGIA

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.

EASTERN EUROPE

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.

SECURITY ORGANIZATIONS

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.

Targeting: Caucasus Region Militaries and Media

- Georgian military
- Armenian military
- Kavkaz Center

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

Targeting: Eastern Europe

- Ministry of Foreign Affairs in Southern EE infected
- Polish government targeted with CORESHELL
  - MH17 lure
- Baltic Host exercises

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.

Targeting: Eastern Europe

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)**

Targeting: European Security Organizations

- NATO
- OSCE

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)**

Targeting: Defense Attaches

- UK
- Turkey
- China
- Japan
- South Korea

Targeting: Wide-ranging Interests

Other probable APT28 targets that we have identified:

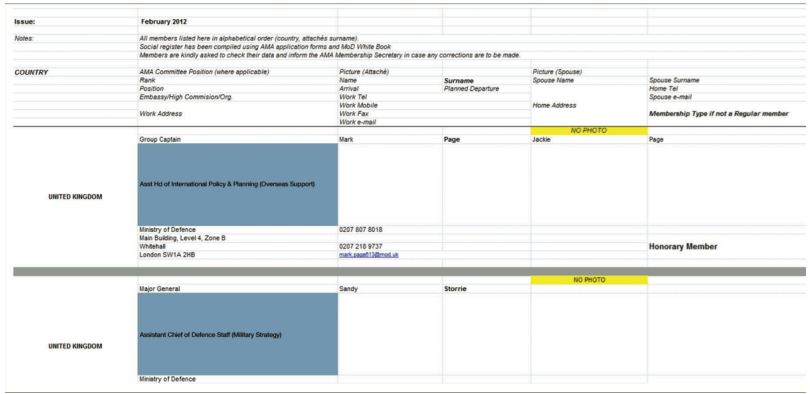
- Norwegian Army (Forsvaret)
- Government of Mexico
- Chilean Military
- Pakistani Navy
- U.S. Defense Contractors
- European Embassy in Iraq
- Special Operations Forces Exhibition (SOFEX) in Jordan
- Defense Attaches in East Asia
- Asia-Pacific Economic Cooperation (APEC)
- Al-Wayi News Site

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

Lures, cont.

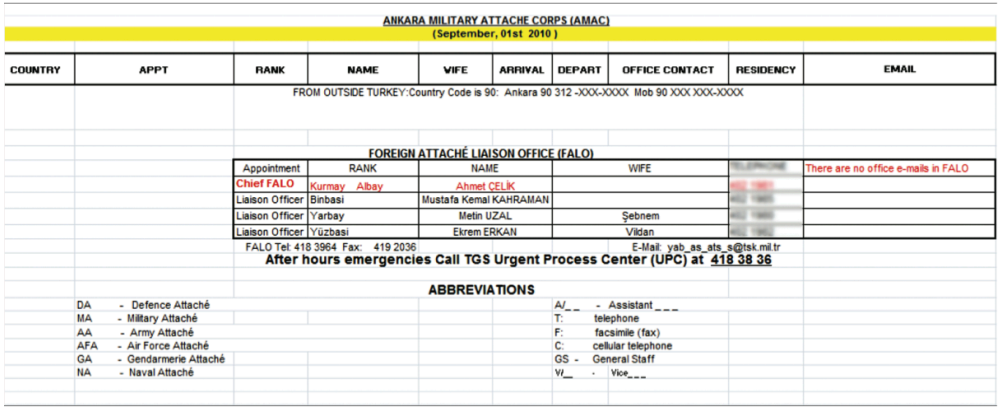
2013	Asia Pacific Economic Cooperation Summit 2013 reporters (internal document)	SOURFACE
2013	Defense Attaches in Turkey (internal document)	CHOPSTICK, CORESHELL
2013	Turkish Cypriot news about Syria chemical weapons	CHOPSTICK, CORESHELL
2013	Georgian language document about drivers' licenses (internal 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



Issue: February 2012

Notes: All members listed here in alphabetical order (country, attachés 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) / Rank / Position / Embassy/High Commision/Org. / Work Address	Picture (Attaché) / Name / Arrival / Work Tel / Work Mobile / Work Fax / Work e-mail	Surname / Planned Departure	Picture (Spouse) / Spouse Name / Home Address	Spouse Surname / Home Tel / Spouse e-mail / Membership Type if not a Regular member
	Group Captain	Mark	Page	Jackie	Page
UNITED KINGDOM	Asst Hd of International Policy & Planning (Overseas Support)			NO PHOTO	
	Ministry of Defence, Main Building, Level 4, Zone B, Whitehall, London SW1A 2HB	0207 807 8018 / 0207 210 9737 / mark.page513@mod.uk			Honorary Member
	Major General	Sandy	Storrie	NO PHOTO	
UNITED KINGDOM	Assistant Chief of Defence Staff (Military Strategy)				
	Ministry of Defence				



ANKARA MILITARY ATTACHE CORPS (AMAC)
(September, 01st 2010)

COUNTRY	APPT	RANK	NAME	WIFE	ARRIVAL	DEPART	OFFICE CONTACT	RESIDENCY	EMAIL

FROM OUTSIDE TURKEY:Country Code is 90: Ankara 90 312 -XXX-XXXX Mob 90 XXX XXX-XXXX

FOREIGN ATTACHÉ LIAISON OFFICE (FALO)

Appointment	RANK	NAME	WIFE		There are no office e-mails in FALO
Chief FALO	Kurmay Albay	Ahmet ÇELİK			
Liaison Officer	Binbasi	Mustafa Kemal KAHRAMAN			
Liaison Officer	Yarbay	Metin UZAL	Şebnem		
Liaison Officer	Yüzbasi	Ekrem ERKAN	Vildan		

FALO Tel: 418 3964 Fax: 419 2036 E-Mail: yab_as_ats_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___

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 Malware Created in Russia?

- More than 50% of the malware samples with Portable Executable (PE) resources included Russian language settings
  - significant portion of APT28 malware was compiled in a Russian language build environment consistently over the course of six years (2007 to 2013)
  - over the time Russian language settings are being replaced by neutral or English language

Russian language in the code

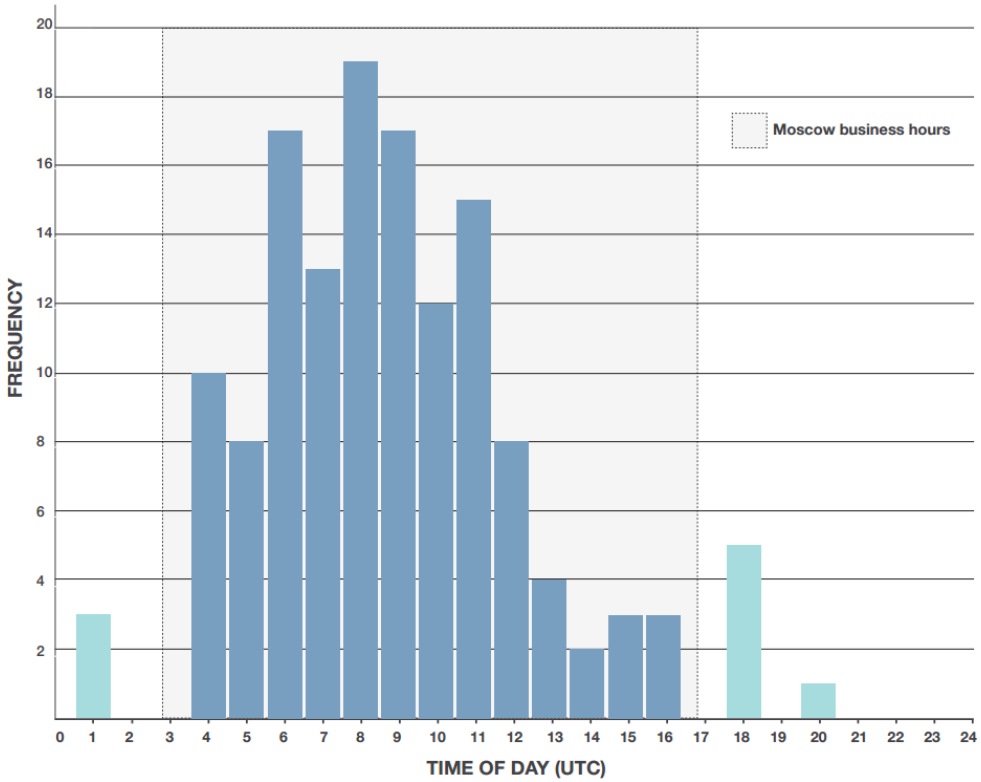
- Locale and language identifiers associated with APT28 malware

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

APT28 Malware Created in Russia?

- Compilation times
  - Over 96% of the malware samples were compiled between Monday and Friday
  - More than 89% were compiled between 8AM and 6PM in the UTC+3 / 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

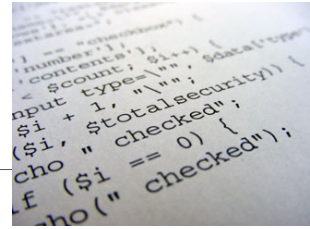
When were developers working?



APT28 Malware Overview

- 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 Malware Overview, cont.



- APT28 tailors implants for specific victim environments.
  - They steal data by configuring their implants to send data out of the network using for example a victim network's mail server.
- Several of APT28's malware samples contain counter-analysis capabilities
  - runtime checks to identify an analysis environment
  - obfuscated strings unpacked at runtime
  - the inclusion of unused machine instructions to slow analysis
  - RSA encryption of stolen data

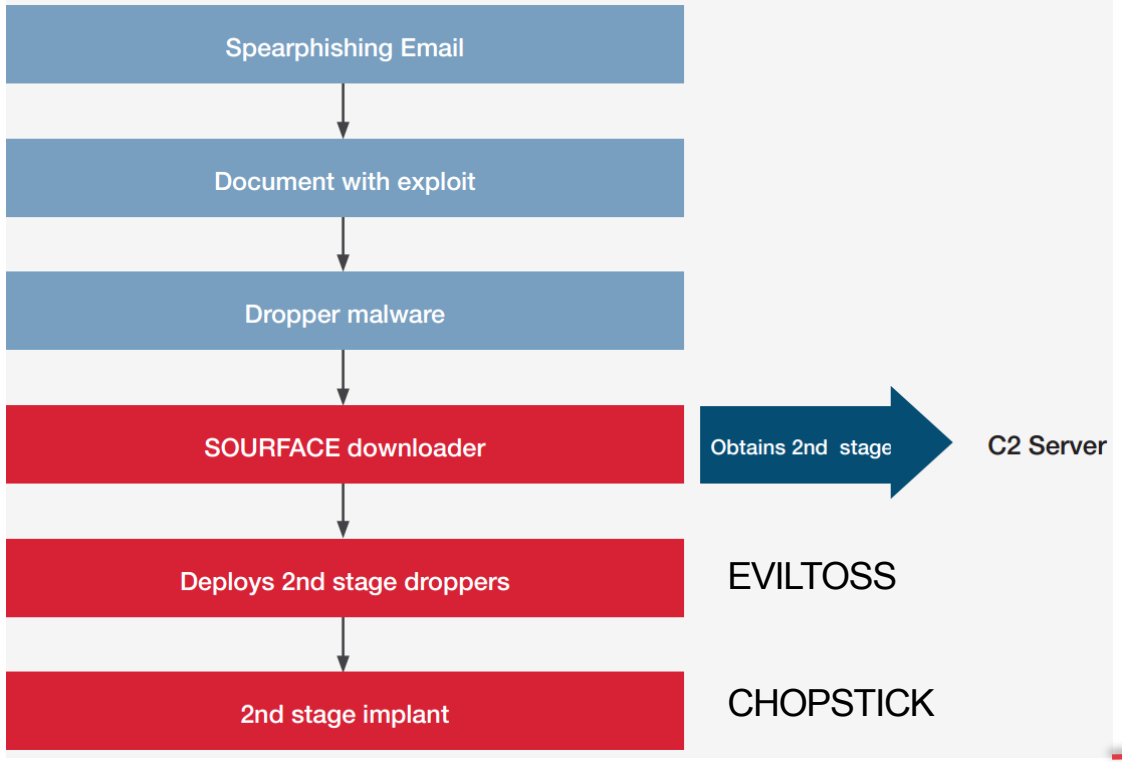
Malware: Ecosystem and Attack Lifecycle

Can be also a compromised web site

Can be also JS/applet based exploit

Obfuscated/encrypted to evade detection

Obfuscated/encrypted to evade detection, dedicated



FireEye

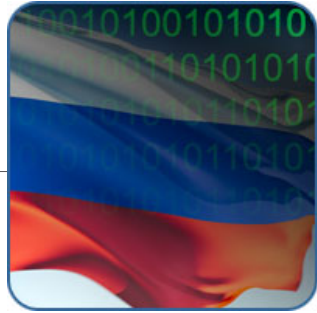
Malware

- 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

Malware, cont.

- CORESHELL
  - It is an updated version of SOURFACE
  - Switched C2 Servers from hardcoded IPs into domains
  - The compiled DLL name changed to `coreshell.dll`
  - Minor changes to the network communications
- EVILTOSS
  - this backdoor has been delivered through the SOURFACE downloader to gain system access for reconnaissance, key logging, monitoring, credential theft, and shellcode execution
  - The backdoor encrypts data that it uploads with an RSA public key
  - Many of its variants we have seen are named `netui.dll`.
  - EVILTOSS variants may use the Simple Mail Transfer Protocol (SMTP) to send stolen data in an attachment named “`detaluri.dat`”

Malware, cont.



- CHOPSTICK
  - This is a modular implant compiled from a software framework that provides tailored functionality and flexibility (for example to use local network resources such as email server)
  - CHOPSTICK variant contained modules and functions for collecting keystroke logs, Microsoft Office documents, and PGP files
- CHOPSTICK variants may move messages and information using:
  1. Communications with a C2 server using HTTP
  2. Email sent through a specified mail server. All information required for the email was hardcoded in the backdoor.
  3. Local copying to defeat closed networks by routing messages between local directories, the registry and USB drives

Malware, cont.

- OLDBAIT
  - It is a credential harvester
  - Installs itself in `%ALLUSERPROFILE%\\Application Data\Microsoft\MediaPlayer\updatewindws.exe`
  - Credentials for the following applications are collected: Internet Explorer, Mozilla Firefox, Eudora, The Bat! (an email client), Becky! (an email client)
  - Both email and HTTP can be used to send out the collected credentials

Malware: Updated Since 2007

- New network traffic formats, export functions, filenames
- Removed Russian language resources
- The hostname, volume serial number and OS version data are encoded in the new URL format.

Example of modified SOURFACE vs. CORESHELL communications

SOURFACE 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==
```

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+sq2m1a5HcqyC5Zd6yrC2WNYL989WCHse9qO6c7powrOUh5KY=
```

Conclusion

- FireEye started researching APT28 based on activity we observed on our clients' networks, similar to other targeted threat groups we have identified over time
- 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

Additional Information

- FireEye Blog

https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html

- Indicators (IOC) to help organizations detect APT28 activity

https://github.com/fireeye/iocs

Questions?