ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

Protection of Clouds against Targeted Attacks

Alexander Adamov
NioGuard Security Lab,
Kharkiv National University of Radio Electronis

IM&CTCPA 2016, 31.10-02.11.2016

Problem

Detection of targeted attacks[1]

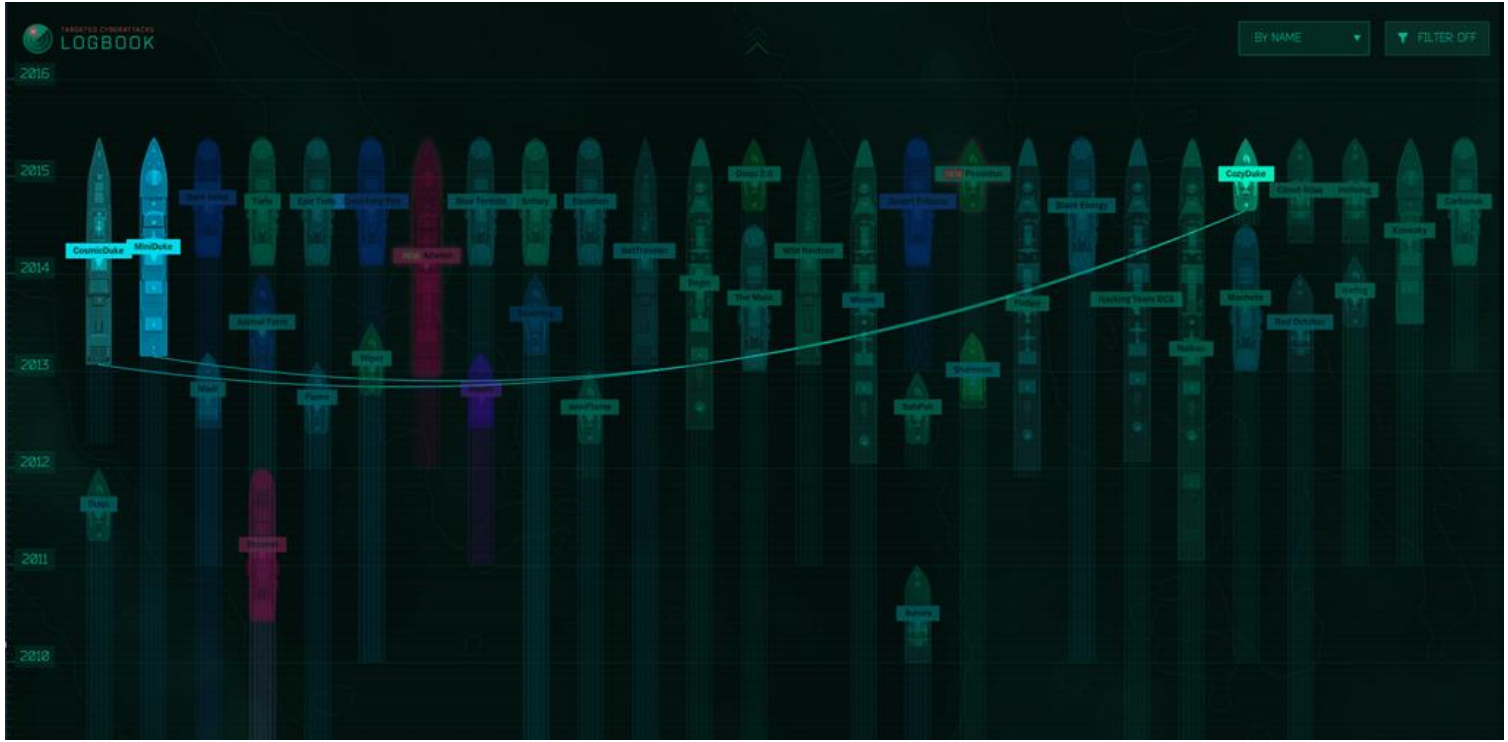
- cyber weapon (Stuxnet)
- cyber espionage (APT Duke and Turla espionage campaigns)
- cyber robbery ($1 billion bank robbery with APT Carbanak)
- ransomware (cryptolockers: TeslaCrypt, CryptXXX, Petya&Misha)

The majority of mass market antiviruses and IDS/IPS solutions misses targeted attacks[2]

[1] Targeted attacks have the low number of infections and can hiddenly operate for a long time. Because of that, they are called *Advanced Persistent Threats (APT)*.

[2] IDS/IPS including antiviruses in the majority cases are unaware of APTs as they detect mostly already discovered threats. APTs use self-defense techniques: obfuscation, polymorphic encryption, digital signatures to bypass antivirus protection. In advance, Watering hole, spear-phishing, and 0-day exploits are used to penetrate a security perimeter of an organization.

Chronology of Targeted Attacks

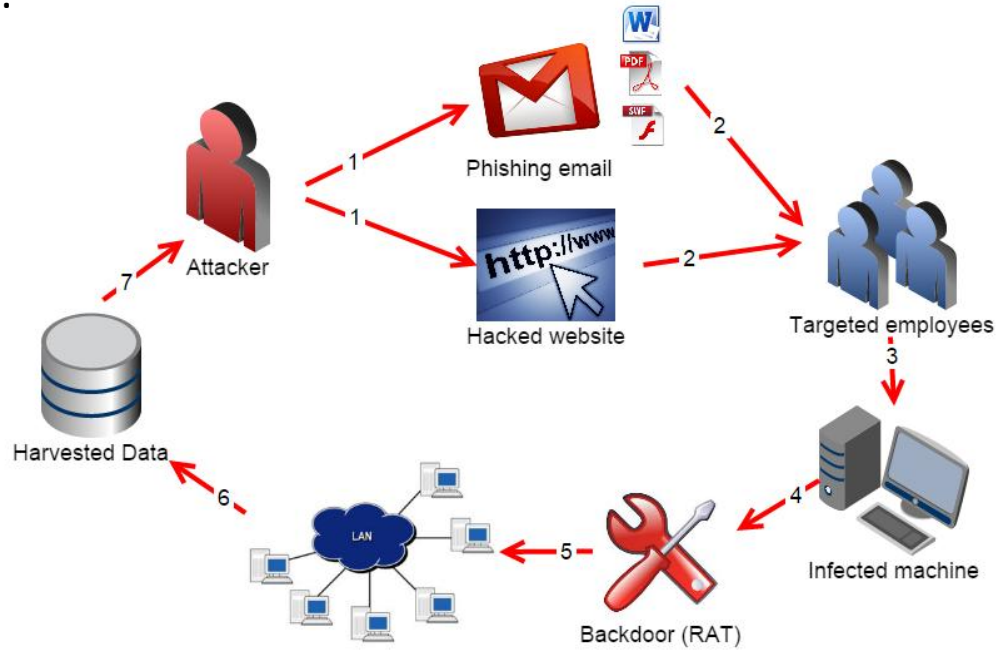


Source: https://apt.securelist.com/

A model of targeted attack

Targeted attacks can be executed via:

a. spear-phishing emails
b. watering hole attacks
c. 0-day exploits



Duke Family

APT* “CosmicDuke/MiniDuke” – July 2014

The malware can steal a variety of information, including files based on extensions and file name keywords:

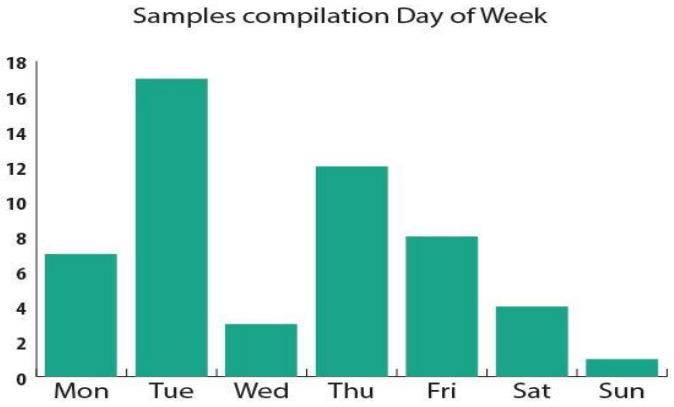
***.exe;*.ndb;*.mp3;*.avi;*.rar;*.docx;*.url;*.xlsx;*.pptx;*.ppsx;*.pst;*.ost;*psw*;*pass*; *login*;*admin*;*sifr*;*sifer*;*vpn;*.jpg;*.txt;*.lnk; *.dll;*.tmp;*.obj;*.ocx;*.js**

The backdoor equipped with the following capabilities:

– Keylogger – Skype password stealer – General network information harvester – Screen grabber (grabs images every 5 minutes) – Clipboard grabber (grabs clipboard contents every 30 seconds) – Microsoft Outlook, Windows Address Book stealer – Google Chrome password stealer – Google Talk password stealer – Opera password stealer	– TheBat! password stealer – Firefox, Thunderbird password stealer – Drives/location/locale/installed software harvester – WiFi network/adapter information harvester – LSA secrets harvester – Protected Storage secrets harvester – Certificate/private keys exporter – URL History harvester – InteliForms secrets harvester – IE Autocomplete, Outlook Express secrets harvester – and more...

“CosmicDuke” Builds

- 7 builds per day in average



- Uses polymorphic encryption by UPolyXv05_v6 to harden AV detection.

- Spoofs legitimate applications

“CosmicDuke” Victims

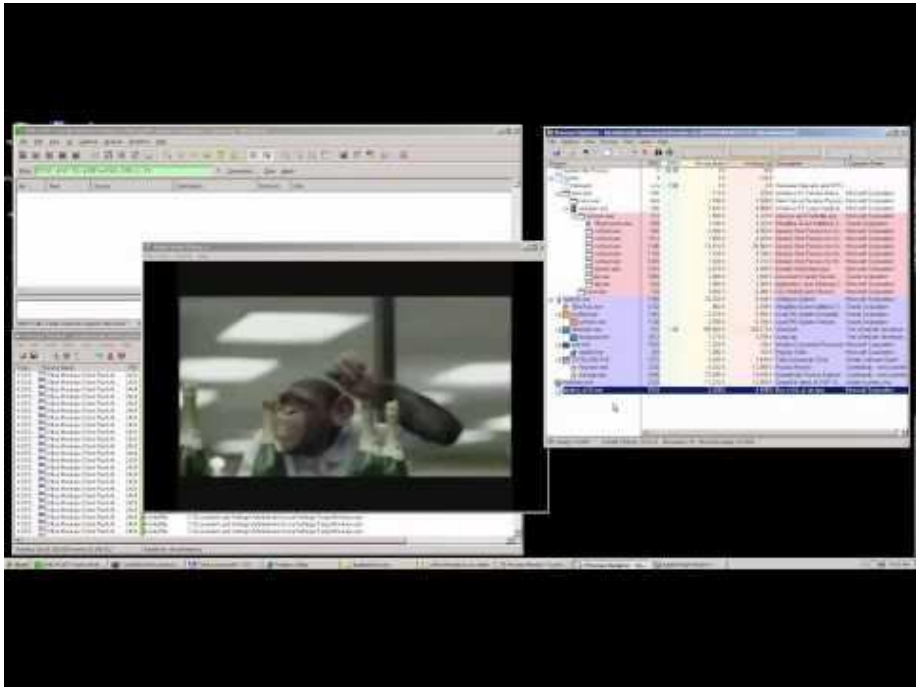
The victims of “CosmicDuke” fall into these categories:

- government
- diplomatic
- energy
- telecom operators
- military, including military contractors
- individuals involved in the traffic and selling of illegal and controlled substances

“CozyDuke”

CozyDuke APT was used to successfully attack the White House and US State Department

The “*Office Monkeys*” viral flash video with a backdoor was sent to employees who then helped to spread it within an organization.



Analysis in Sandbox

Old CosmicDuke 2013

- MD5: edf7a81dab0bf0520bfb8204a010b730

  Download report

New CosmicDuke 2014:

- NVIDIA WLMerger App, MD5: 1276d0aa5ad16fb57426be3050a9bb0b

  Download report

- Adobe Acrobat Updater, MD5: d92faef56fa25120cb092f1b69838731

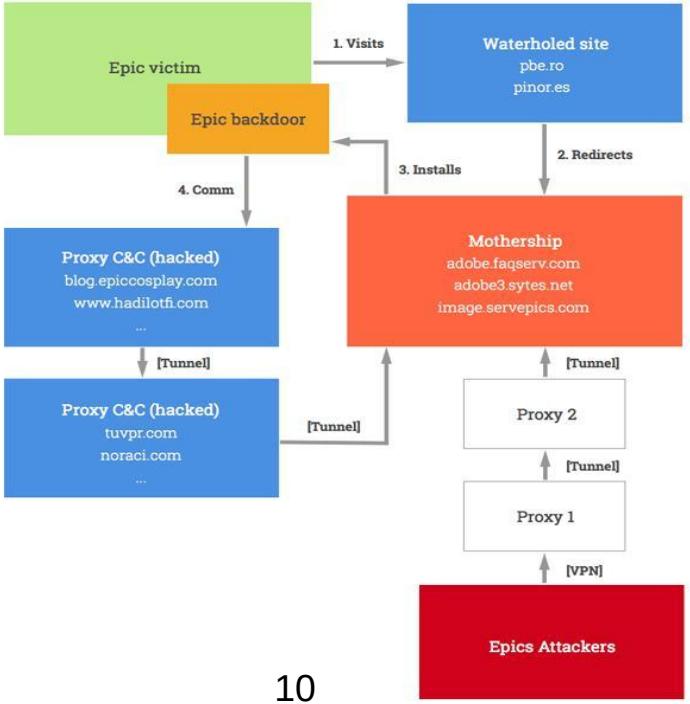
  Download internal report

The “Epic Turla” Attack

“Epic Turla” – is a massive cyber espionage operation.

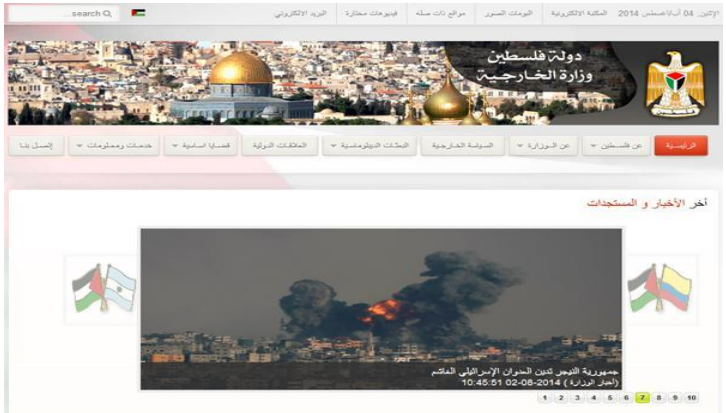
The attackers behind Epic Turla have infected several hundreds computers in more than 45 countries, including:

- government institutions
- embassies
- military
- education
- research and pharmaceutical companies



“Epic Turla” infection vectors

- Spearphishing e-mails with Adobe PDF exploits (CVE-2013-3346 + CVE-2013-5065)
- Social engineering to trick the user into running malware installers with ".SCR" extension, sometimes packed with RAR
- Watering hole attacks using Java exploits (CVE-2012-1723), Flash exploits (unknown) or Internet Explorer 6,7,8 exploits (unknown)
- Watering hole attacks that rely on social engineering to trick the user into running fake "Flash Player" malware installers.




```
<div style="text-align: left;">
<table style="width: 940px;" border="0">
<tbody>
<tr>
<td style="text-align: right;" valign="top"><strong style="text-align: right;"><span style="color: #ff0000;"
<td>جميع الحقوق محفوظة © 2005 - 2013 وزارة الخارجية الفلسطينية<br />12 م و جوجل كروم +5.0.3 سفاري
</tr>
</tbody>
</table>
</div>
<div><br /> </div>
<div style="text-al
</div><script  src="http://adobe.faqserv.com/macromedia/get/shockwave/latest/sitenavigation.js"></script>

        </div>
    </div>


</body>
```

Watering Hole example:
Infected *Palestinian Authority Ministry of Foreign Affairs*

Analysis in Sandbox

- Adobe PDF Exploits (Note_№107-41D.pdf CVE-2013-5065)

  PDF MD5: 6776bda19a3a8ed4c2870c34279dbaa9 Download report

  – Dropped file (Epic/Tavdig/Wipbot backdoor), MD5: 111ed2f02d8af54d0b982d8c9dd4932e

    Download report

- Spearphishing files:

  – NATO position on Syria.scr, MD5: 4d667af648047f2bd24511ef8f36c9cc

    Download report

    - Dropped Epic/Tavdig/Wipbot backdoor, MD5: ab686acde338c67bec8ab42519714273

      Download report

- Turla Carbon package

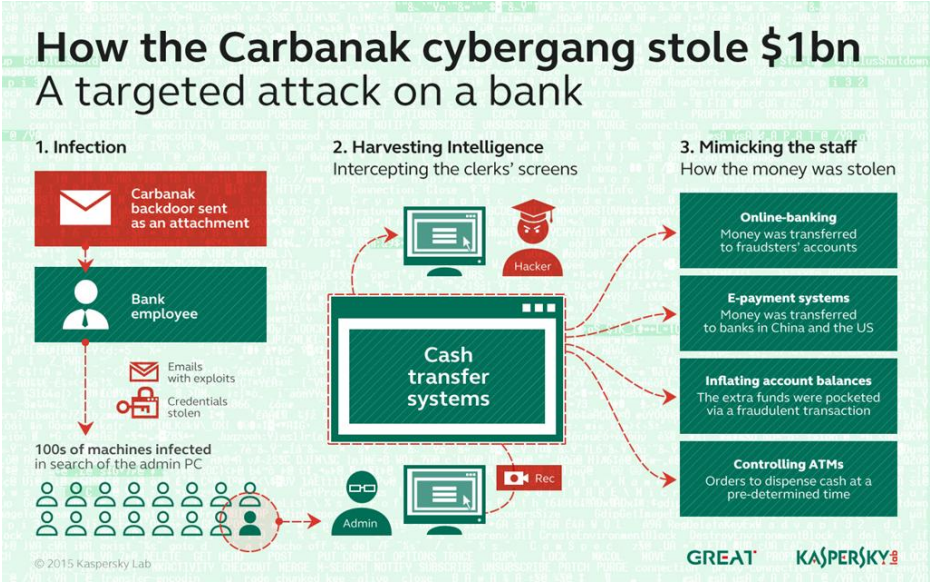
  MD5: cb1b68d9971c2353c2d6a8119c49b51f Download report

Carbanak APT

- Up to 100 financial institutions have been hit.Total financial losses could be as a high as $1bn
- Each bank robbery took 2-4 months, from infecting the first computer to cashing the money out
- Losses from #Carbanak per bank range from $2.5 million to approximately $10 million

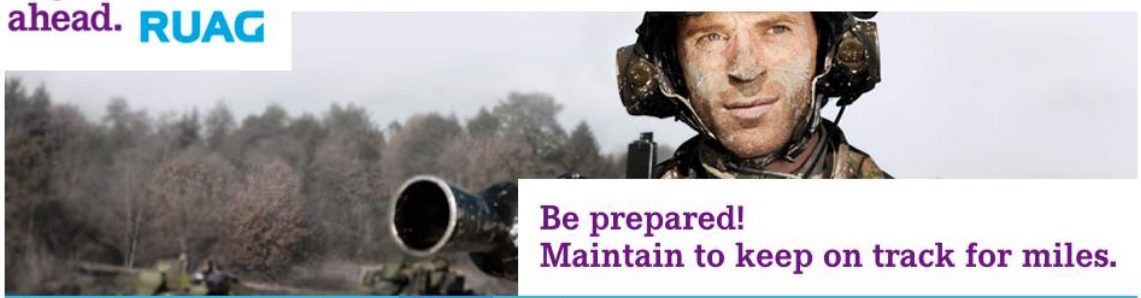
Analysis in Sandbox:

MD5: 4afafa81731f8f02ba1b58073b47abdf
MD5: 551d41e2a4dd1497b3b27a91922d29cc



APT case RUAG

Together ahead. RUAG



Group | Space | Aviation | Aerostructures | Defence | Ammotec

Defence Home | Land Systems | Network Enabled Operation Services | Simulation & Training

About us
Media
Certifications
Career
Events
Locations
Contact

Media release

Back to overview

12.05.2016 | RUAG Group

Cyber attack on RUAG: major damage averted

Berne, 12 May 2016. Cybercrime strikes Switzerland: RUAG has considerable IT expertise and many years of successful experience in the security field. Nevertheless, there is no such thing as 100% security. With the support of federal agencies, an attack on RUAG has been detected and halted. Further damage has thus been averted.

Inquiries to:

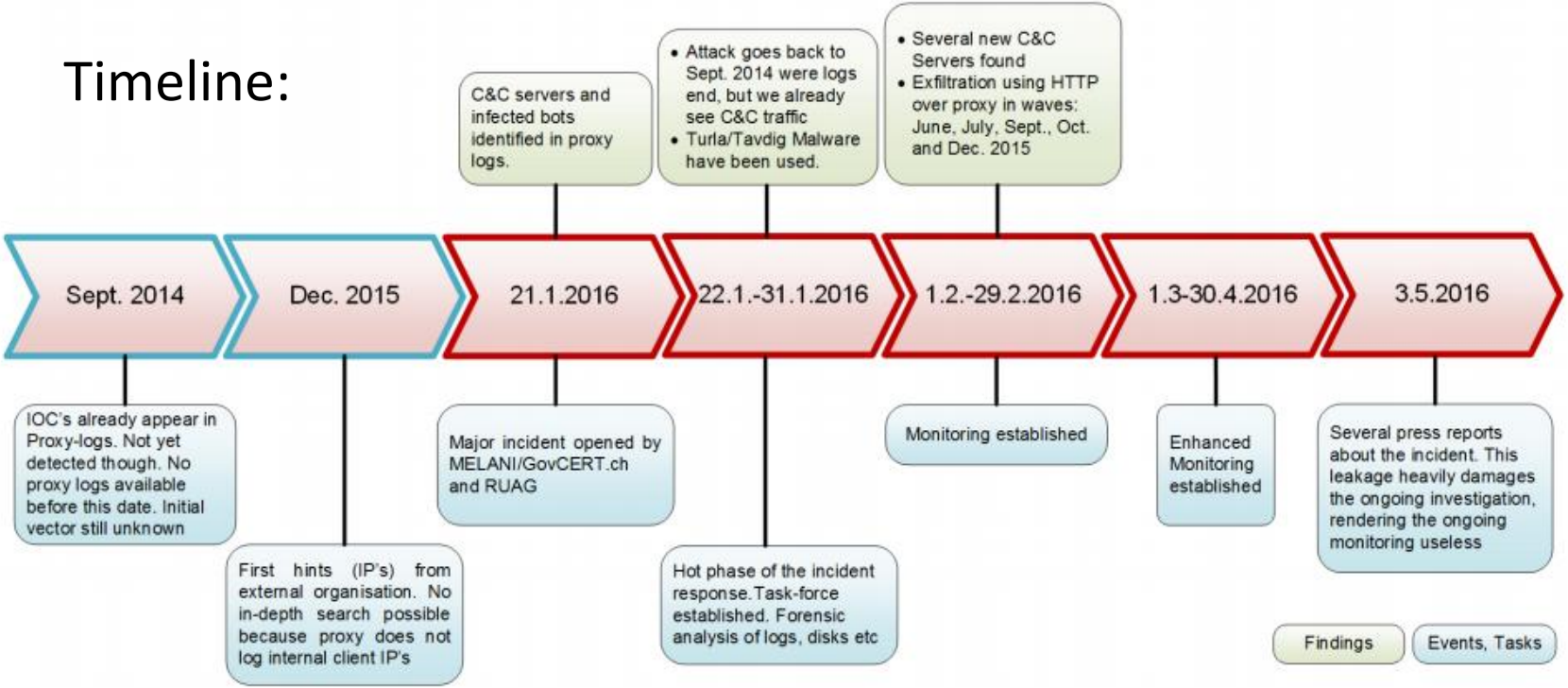
RUAG Corporate Services AG
Schaffhauserstrasse 580
8052 Zürich - Schweiz

Jiri Paukert

Senior Manager External Communication
+41 79 758 47 77

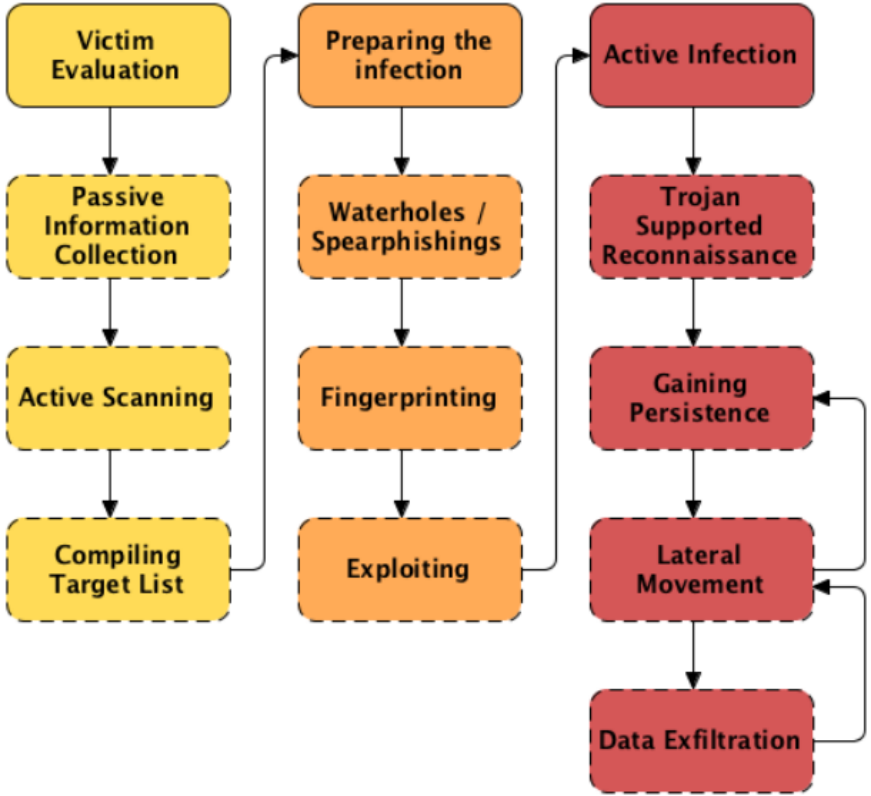
APT case RUAG

Timeline:



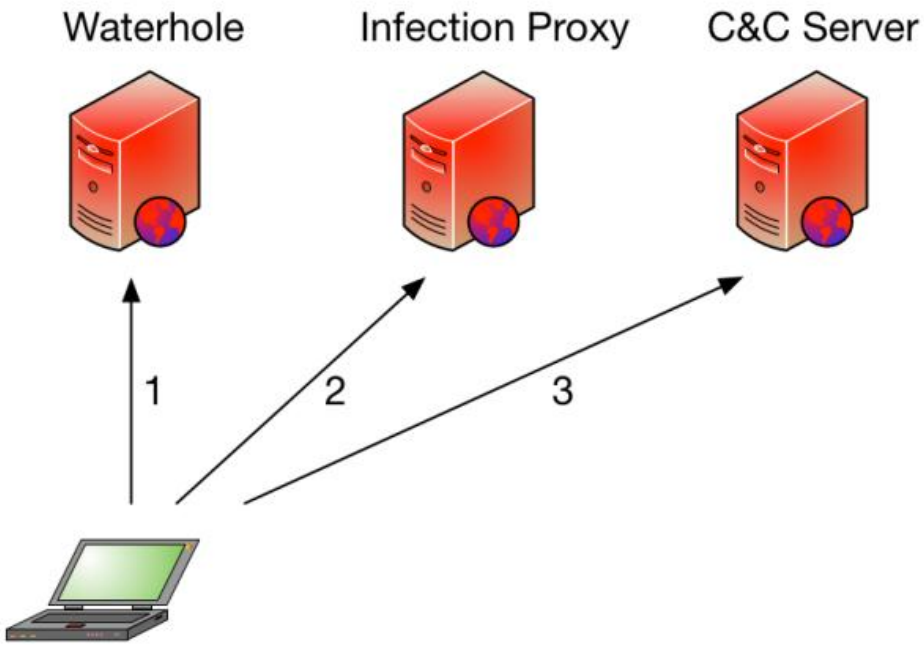
APT case RUAG

Phases of the attack:



APT case RUAG

Infection:



APT Backdoors

- **PlugX**
  - MD5: d376f29dc8a1c6fd4b8849c9d57e3e03

- **BlackEnergy**
  - MD5: 3fa9130c9ec44e36e52142f3688313ff

Overview of Cryptolockers

- Android.SimpleLocker
- Linux.Cryptor
- NanoLocker
- VaultCrypt
- TeslaCrypt
- Petya & Misha

VaultCrypt

Delivery method:	via spam messages with a malicious javascript attachment
Platform/ File type:	Windows/BAT
Files encryption method:	RSA-1024 using the GnuPG tool
Session key encryption method:	RSA-1024 with the hard-coded master public key using GnuPG tool
Encryption locations:	files are not encrypted in the folders: Windows, msoffice, Intel, and framework64
Deleting backup:	yes, using SDelete or Cipher tools to wipe the keys files
Communication with C&C server:	http://revault.me
Decryption service:	in Tor network
Payment:	in BTC, the price depends on the number of encrypted files
Targeted audience:	Russian speaking (Russia, Ukraine)
Passive methods of protection:	n/a
Active methods of protection:	n/a

TeslaCrypt

Delivery method:	landed via a drive-by attack with the help of the Angler web exploit
Platform/ File type:	Windows/EXE
Files encryption method:	AES-256-CBC using the OpenSSL library code
Session key encryption method:	the key is used as a multiplier in the calculated ECDH shared secret sent to the C&C server and stored in a header of encrypted files
Encryption locations:	Exceptions: Windows, Program Files, and Application Data. Encrypted in shared folders and removable drives
Deleting backup:	yes, using vssadmin.exe [11] to delete shadow copies of files
Communication with C&C server:	URL varies on the build version, data transmitted in an encrypted way (AES-256-CBC) with the hard-coded key
Decryption service:	in Tor network
Payment:	$500 equivalent in BTC, doubled every 60 hours
Targeted audience:	English speaking
Passive methods of protection:	polymorphic encryptor
Active methods of protection:	n/a

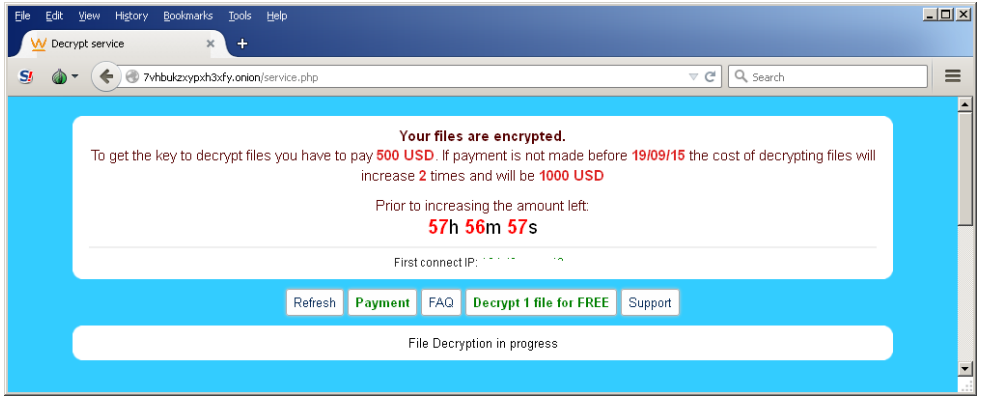
TeslaCrypt 2.1

- Analysis of TeslaCrypt 2.1

  http://nioguard.blogspot.se/2015/09/teslacrypt-21-analysis-cracking-ping.html

- NAS report:

  Search on http://nas.nioguard.com/ by MD5: b10d45335b8de97e6bc1d5cc9449c323



NanoLocker

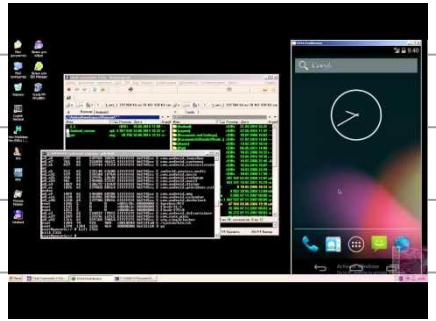
Delivery method:	n/a
Platform/ File type:	Windows/EXE
Files encryption method:	AES-256-CBC using the Windows Enhanced Cryptographic Provider (RSAENH)
Session key encryption method:	RSA-1024 with the hard-coded master public key and base64 encoded to be sent via a Public Note in a Bitcoin transaction
Encryption locations:	no exceptions
Deleting backup:	no
Communication with C&C server:	ICMP, two ping packets are sent with a Bitcoin address to C&C (52.91.55.122), the second ping packet is sent once the encryption is completed and also contains the number of encrypted files
Decryption service:	using a Public Note in Bitcoin transaction
Payment:	0.25 BTC
Targeted audience:	English speaking
Passive methods of protection:	packing, base64
Active methods of protection:	n/a

Linux.Cryptor

Delivery method:	via exploitation of a vulnerability in the Magento platform to launch attacks on web servers
Platform/ File type:	Linux/ELF
Files encryption method:	AES-128-CBC using the PolarSSL library
Session key encryption method:	RSA-1024 with the hard-coded master public key
Encryption locations:	files are encrypted in the folders: /home, /root, /var/lib/mysql, /var/www, /etc/nginx, /etc/apache2, /var/log
Deleting backup:	n/a
Communication with C&C server:	n/a
Decryption service:	in Tor network
Payment:	1 BTC
Targeted audience:	English speaking
Passive methods of protection:	n/a
Active methods of protection:	n/a

SimpleLocker

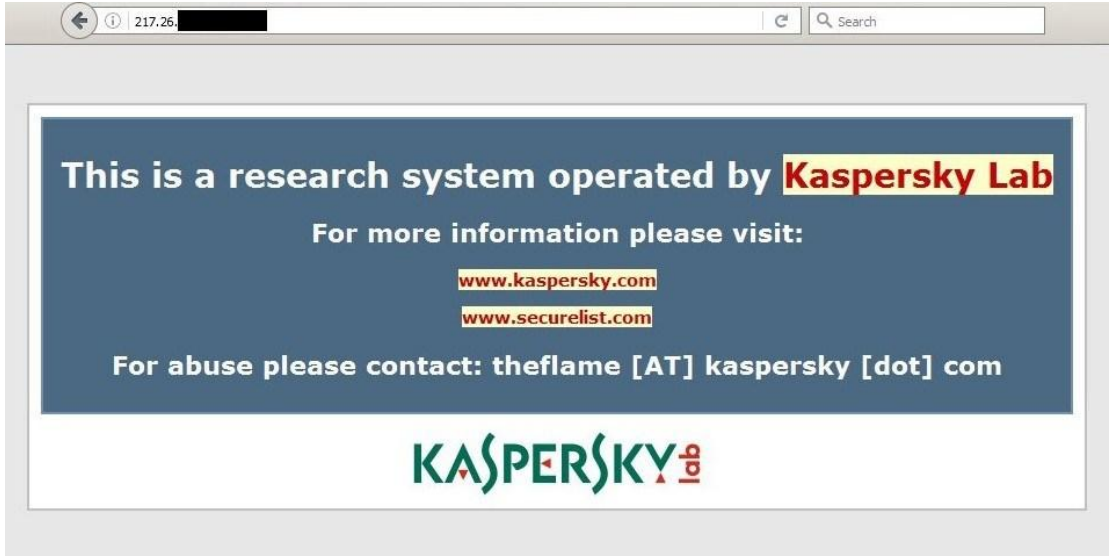
Delivery method:	downloaded from unofficial Android app stores as a fake porn game
Platform/ File type:	Android/APK
Files encryption method:	AES-128-CBC using the cryptolib
Session key encryption method:	the files encryption key is hard-coded "jndlasf074hr"
Encryption locations:	files on an SD card
Deleting backup:	n/a
Communication with C&C server:	in Tor (http://xeyocsu7fu2vjhxs.onion/), user's data are transmitted in JSON format
Decryption service:	the decrypting routine is available in the cryptolocker's code
Payment:	MoneXy, Qiwi
Targeted audience:	Ukraine
Passive methods of protection:	code obfuscation in some versions
Active methods of protection:	n/a



https://youtu.be/dFXqMFsgutg?t=32

Delivery Method “I have a pen”

A malicious website delivering Petya ransomware through the Hunter exploit kit. https://securelist.com/blog/incidents/76357/trust-me-i-have-a-pen/



Nemucod Cryptolocker

Malicious URLs

Congratulations

You have just one $57,576 due to your winning Binary trade account.

> Collect your winnings HERE <

Or alternatively use your winnings and make more money by clicking the link below.

MAKE MORE CASH HERE

These are your winnings from the total month of April.

Thanks

Support Team

“ATTENTION!

All your documents, photos, databases and other important personal files were encrypted using strong RSA-1024 algorithm with a unique key.

To restore your files you have to pay 0.52985 BTC(bitcoins).

Please follow this manual:

...

Source: http://sensorstechforum.com/remove-nemucod-ransomware-and-restore-crypted-encrypted-files/

Nemucod Cryptolocker

```
000000: FF D8 FF E1 39 E0 45 78 |ÿØÿá9àEx
000008: 69 66 00 00 49 49 2A 00 |if  II*
000010: 08 00 00 00 08 00 0F 01 |◘   ◘ ☼.
000018: 02 00 12 00 00 00 6E 00 |┐ ↕   n
000020: 00 00 10 01 02 00 0B 00 |  ┼.┐ ♂
000028: 00 00 80 00 00 00 1A 01 |  €   →.
000030: 05 00 01 00 00 00 8C 00 |│ .   Œ
000038: 00 00 1B 01 05 00 01 00 |  ←.│ .
000040: 00 00 94 00 00 00 28 01 |  ″   (.
000048: 03 00 01 00 00 00 02 00 |└ .   ┐
000050: 00 00 31 01 02 00 28 00 |  1.┐ (
000058: 00 00 9C 00 00 00 32 01 |  œ   2.
000060: 02 00 14 00 00 00 C4 00 |┐ ¶   Ä
000068: 00 00 69 87 04 00 01 00 |  i‡┘ .
000070: 00 00 D8 00 00 00 6E 03 |  Ø   n└
000078: 00 00 4E 49 4B 4F 4E 20 |  NIKON
000080: 43 4F 52 50 4F 52 41 54 |CORPORAT
000088: 49 4F 4E 00 4E 49 4B 4F |ION NIKO
000090: 4E 20 44 36 30 30 00 00 |N D600
000098: 2C 01 00 00 01 00 00 00 |,.  .
0000A0: 2C 01 00 00 01 00 00 00 |,.  .
```

```
000000: CE BA 6C 69 F5 F0 A2 4C |Î°liõð¢L
000008: E8 56 7C C8 B3 65 74 D6 |èV|È³etÖ
000010: 47 C8 CA 30 9E 38 70 C7 |GÈÊ0ž8pÇ
000018: 1A 70 DA D4 36 98 39 BC |→pÚÔ6˜9¼
000020: 21 94 DB 03 B2 20 9B 44 |!”Û└² ›D
000028: 92 E0 01 F0 5F 30 B9 17 |’à.ð_0¹┤
000030: 67 A4 E7 F0 28 60 6A 28 |g¤çð(`j(
000038: 6A 90 FF 39 5C 8E C2 5C |jÿ9\ŽÂ\
000040: A6 F0 0E 10 86 C8 D3 2F |¦ð♫┼†ÈÓ/
000048: 2E 62 96 3A 8B DC 8E F0 |.b–:‹ÜŽð
000050: 54 94 36 7B D3 16 73 D4 |T”6{Ó┬sÔ
000058: 4A C0 F6 C0 16 A0 E7 0B |JÀöÀ┬ ç♂
000060: 04 4C 86 F0 68 E0 F5 62 |┘Lðhàõb
000068: 93 88 A5 97 E3 34 80 30 |“ˆ¥—ã4€0
000070: 7C C8 22 2C 5E D6 21 CB |│È",^Ö!Ë
000078: CA 30 D8 71 34 89 56 50 |Ê0Øq4‰VP
000080: 8B 9B 64 C8 18 EE 60 C0 |‹›dÈ↑î`À
000088: 82 4D FE 20 DE 0D D9 AF |‚Mþ Þ♪Ù¯
000090: CF D0 1B 06 93 26 62 A4 |ÏÐ←♠“&b¤
000098: CA F1 28 60 E7 28 6A 90 |Êñ(`ç(j
0000A0: C8 39 59 8E C2 5C A6 F0 |È9YŽÂ\¦ð
```

...

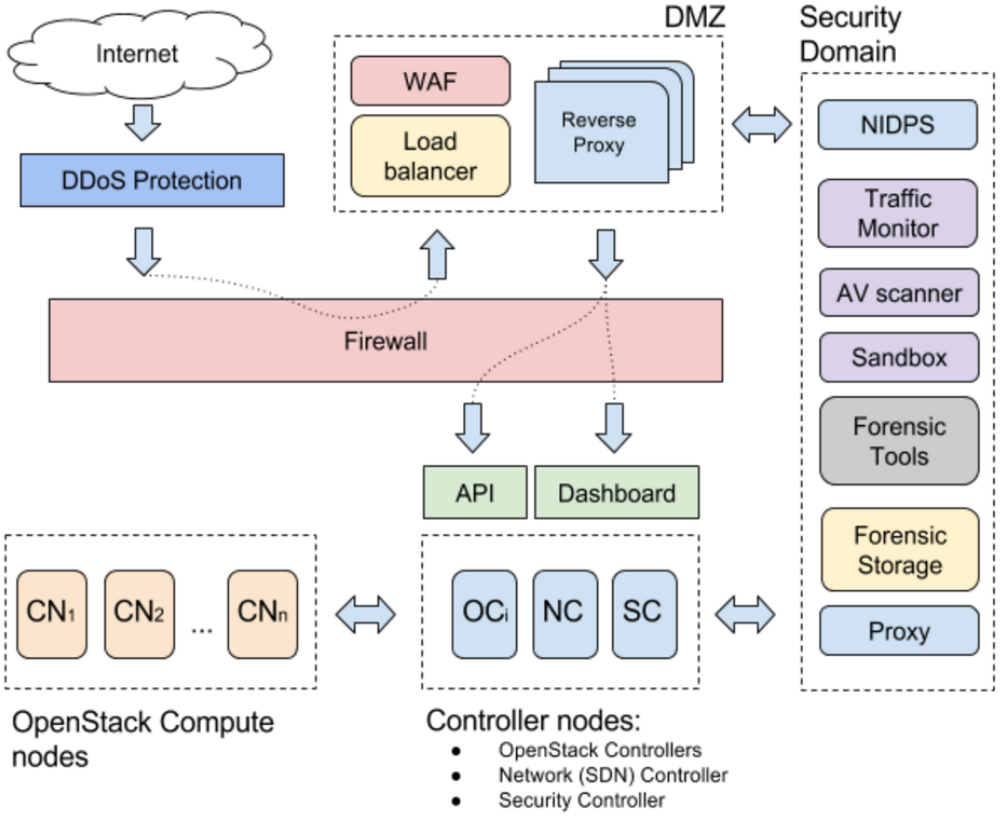
```
0003D0: 48 00 00 00 01 00 00 00 |H   .
0003D8: FF D8 FF DB 00 84 00 06 |ÿØÿÛ „ ♠
0003E0: 04 04 04 05 04 06 05 05 |┘┘┘│┘─││
0003E8: 06 09 06 05 06 09 0B 08 |♠.♠│♠.♂◘
0003F0: 06 06 08 0B 0C 0A 0A 0B |♠♠◘♂♀..♂
0003F8: 0A 0A 0C 10 0C 0C 0C 0C |..♀►♀♀♀♀
000400: 0C 0C 10 0C 0C 0C 0C 0C |♀♀►♀♀♀♀♀
000408: 0C 0C 0C 0C 0C 0C 0C 0C |♀♀♀♀♀♀♀♀
000410: 0C 0C 0C 0C 0C 0C 0C 0C |♀♀♀♀♀♀♀♀
000418: 0C 0C 0C 0C 0C 0C 0C 01 |♀♀♀♀♀♀♀.
000420: 07 07 07 0D 0C 0D 18 10 |•••♪♀♪↑►
000428: 10 18 14 0E 0E 0E 14 14 |►↑¶♫♫♫¶¶
000430: 0E 0E 0E 0E 14 11 0C 0C |♫♫♫♫¶◄♀♀
```

```
0003D0: AC 38 59 8E C2 5C A6 F0 |¬8YŽÂ\¦ð
0003D8: 65 C8 79 13 FB AA 2D 64 |eÈy‼ûª-d
0003E0: 93 3E 8F D9 88 F6 51 91 |“>Ù^öQ‘
0003E8: 01 73 D7 13 5D DD 41 C8 |☺s×‼]ÝAÈ
0003F0: 6C C6 1E AB D9 00 0C 47 |lÆ▲«Ù ♀G
0003F8: 98 FA 64 F0 3D 6E 9F 84 |˜ûdð=nŸ„
000400: 0C 0C 10 0C 0C 0C 0C 0C |♀♀►♀♀♀♀♀
000408: 0C 0C 0C 0C 0C 0C 0C 0C |♀♀♀♀♀♀♀♀
000410: 0C 0C 0C 0C 0C 0C 0C 0C |♀♀♀♀♀♀♀♀
000418: 0C 0C 0C 0C 0C 0C 0C 01 |♀♀♀♀♀♀♀☺
000420: 07 07 07 0D 0C 0D 18 10 |•••♪♀♪↑►
000428: 10 18 14 0E 0E 0E 14 14 |►↑¶♫♫♫¶¶
000430: 0E 0E 0E 0E 14 11 0C 0C |♫♫♫♫¶◄♀♀
```

Petya & Misha

Petya & Misha demo https://youtu.be/QJkUwfa1Yvg

Secure Cloud Architecture



Source: https://docs.mirantis.com/openstack/fuel/fuel-9.1/assets/MirantisSecurityBestPractices.pdf

Demo: IPS as VNF in OpenStack

https://youtu.be/uakDqkKmfiE?t=1249

Contacts

ada@nioguard.com

oleksandr.adamov@nure.ua

@Alex_Ad

Sources

- Targeted Attacks https://apt.securelist.com
- Cloud Security Best Practices https://docs.mirantis.com/openstack/fuel/fuel-9.1/
- OpenStack Security Guide http://docs.openstack.org/security-guide/
- NioGuard Sandbox http://nas.nioguard.com