VIRUS DEFINITION

Virus Type: Advanced Persistent Threat (APT)

What is Epic Turla?

Turla, also known as Snake or Uroburos is one of the most sophisticated ongoing cyber-espionage campaigns. The latest Kaspersky Lab research on this operation reveals that Epic is the initial stage of the Turla victim infection mechanism.

Targets of "Epic" belong to the following categories: government entities (Ministry of Interior, Ministry of Trade and Commerce, Ministry of Foreign/External affairs, intelligence agencies), embassies, military, research and education organizations and pharmaceutical companies.

Most of the victims are located in the Middle East and Europe, however, we observed victims in other regions as well, including in the USA. In total, Kaspersky Lab experts counted several hundred victim IPs distributed in more than 45 countries, with France at the top of the list.

The attacks detected in this operation fall into several different categories depending on the initial infection vector used in compromising the victim:

- Spear-phishing 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), Adobe 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

Threat Details

The attackers use both direct spear-phishing e-mails and watering hole attacks to infect victims. Watering holes are websites commonly visited by potential victims. These websites are compromised in advance by the attackers and injected to serve malicious code. Depending on the visitor's IP address (for instance, a government organization's IP), the attackers serve Java or browser exploits, signed fake Adobe Flash Player software or a fake version of Microsoft Security Essentials.

In total, we have observed more than 100 injected websites. The choice of the websites reflects specific interest of attackers. For example, many of infected Spanish websites belong to local governments.

Once the user is infected, the Epic backdoor immediately connects to the command-and-control (C&C) server to send a pack with the victim's system information. The backdoor is also known as "WorldCupSec", "TadjMakhal", "Wipbot" or "Tadvig".

Once a system is compromised, the attackers receive brief summary information from the victim, and based on that, they deliver pre-configured batch files containing a series of commands for execution. In addition to these, the attackers upload custom lateral movement tools. These include a specific keylogger tool, a RAR archiver and standard utilities like a DNS query tool from Microsoft.

How do I know if I'm infected by the Epic Turla

The best way to determine if you've been a victim of the Epic Turla is to identify if there has been an intrusion. Threat identification can be done with a strong antivirus product such as Kaspersky Lab solutions.

Kaspersky Lab products will detect the following modules of the Epic Turla:

Backdoor.Win32.Turla.an
Backdoor.Win32.Turla.ao
Exploit.JS.CVE-2013-2729.a
Exploit.JS.Pdfka.gkx
Exploit.Java.CVE-2012-1723.eh
Exploit.Java.CVE-2012-1723.ou
Exploit.Java.CVE-2012-1723.ov
Exploit.Java.CVE-2012-1723.ow
Exploit.Java.CVE-2012-4681.at
Exploit.Java.CVE-2012-4681.au
Exploit.MSExcel.CVE-2009-3129.u
HEUR:Exploit.Java.CVE-2012-1723.gen
HEUR:Exploit.Java.CVE-2012-4681.gen
HEUR:Exploit.Java.Generic
HEUR:Exploit.Script.Generic
HEUR:Trojan.Script.Generic
HEUR:Trojan.Win32.Epiccosplay.gen
HEUR:Trojan.Win32.Generic
HackTool.Win32.Agent.vhs
HackTool.Win64.Agent.b
Rootkit.Win32.Turla.d
Trojan-Dropper.Win32.Dapato.dwua
Trojan-Dropper.Win32.Demp.rib
Trojan-Dropper.Win32.Injector.jtxs
Trojan-Dropper.Win32.Injector.jtxt
Trojan-Dropper.Win32.Injector.jznj
Trojan-Dropper.Win32.Injector.jznk
Trojan-Dropper.Win32.Injector.khqw
Trojan-Dropper.Win32.Injector.kkkc
Trojan-Dropper.Win32.Turla.b
Trojan-Dropper.Win32.Turla.d
Trojan.HTML.Epiccosplay.a
Trojan.Win32.Agent.iber
Trojan.Win32.Agent.ibgm
Trojan.Win32.Agentb.adzu
Trojan.Win32.Inject.iujx
Trojan.Win32.Nus.g
Trojan.Win32.Nus.h

How can I protect myself against The Epic Turla

- Keep operating system and all third party applications, notably Java, Microsoft Office and Adobe Reader updated
- Do not install software from untrusted sources, for instance when prompted by a random page
- Be wary of e-mails from unknown sources containing suspicious attachments or links

A security solution should be turned on at all times and all its components should be active. The solution's databases should also be up to date

Other related articles and links related to Malware Threats

- The Onion Ransomware (Encryption Trojan)
- Crouching Yeti Malware Threat
- Kaspersky Internet Security

Featured Articles


What's the Difference between a Virus and a Worm?


Top 7 Mobile Security Threats in 2020


Malware & Computer Virus Facts & FAQs


Top 10 Most Notorious Hackers of All Time


Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online