Critical Threat Alert 1. 2013

ICEFOG: THREAT ANALYSIS AND DEFENSE STRATEGY

THE CRITICAL THREAT ALERT SERIES FROM KASPERSKY

http://www.kaspersky.com/business-security

KASPERSKY lab

Icefog: Threat analysis and defense strategy.

A Critical Threat Alert from Kaspersky

Kaspersky Lab researchers have discovered yet another Advanced Persistent Threat (APT). "**Icefog**"[1] targets government institutions, military contractors, and industrial organizations, mostly in Japan and South Korea.

The Icefog backdoor uses standard techniques to infiltrate its targets: spear phishing emails deliver a set of exploits focused on vulnerabilities in popular software such as Microsoft Office and Java. The global popularity of these applications has motivated cybercriminals to analyse their code for vulnerabilities that allow them to exploit and infect targets. Icefog's creators have enthusiastically harvested the fruits of this research to launch attacks at will.

The exploits used in these attacks are not so-called 'Zero Days' — dangerous exploits unknown to software developers — **these are widely known vulnerabilities and patches are available for them.**

It's one thing to have patches available, but prompt application of them is another matter. Patching is a critical task for systems administrators, particularly those working on government or industrial infrastructure organizations. In these contexts, maximum availability and process protection often get priority over information security. In some instances, administrators prefer not to apply patches at all, for fear of causing latency or instability elsewhere in their systems. Others may lack the time or inclination, particularly in large infrastructures where patching is done manually and some workstations are easily overlooked. Cybercriminals are fully aware of this. That's why an effective targeted attack like Icefog doesn't necessarily require the development of sophisticated zero-day exploits.

[1] Source: http://www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers

How can we minimize the risk of falling prey to an APT like this? First, take advantage of existing technologies that can reinforce your infrastructure against known exploits. Patch Management and Vulnerability Assessment technologies offer an ideal symbiotic approach to protection against known exploits.

Vulnerability Assessment [2] technology addresses this type of threat by tracking and detecting known vulnerabilities in software applications, including operating systems and widely used 3rd party applications, such as Microsoft Office, Java-based applications, Adobe Flash/Acrobat and others.

Kaspersky Lab's Vulnerability Assessment technology is built around a substantial product database that draws on data generated by our unique information stream, developed and analysed by Kaspersky Lab experts. This in-house data, which is the largest source for our vulnerability database, comes from the Kaspersky Security Network — a constantly updated stream of intelligence about vulnerabilities and malware derived from scanning millions of computers all over the world. This data is assessed by Kaspersky Lab's systems and malware experts before being added to the global vulnerabilities database.

Patch management technology helps to monitor, download and apply operating system and, more importantly, 3rd party application patches. Kaspersky's technology can enable the automatic patching of vulnerabilities as soon as 3rd party vendors make them available; the sooner patches are implemented, the easier it is to stay ahead of targeted malware using known explots. Kaspersky's patch management supports the scheduling of patch distribution, allowing administrators to prioritize patches based on importance or criticality. Patches can also be tested in isolation prior to deployment on the whole network. Independent test results[3] confirm the quality of Kaspersky's patch management solution.

[2] Source: http://eugene.kaspersky.com/2013/03/05/kaspersky-systems-management/
[3] Source: http://media.kaspersky.com/pdf/AV-Test-Kaspersky-PM.pdf

But what if an attacker discovers a zero-day vulnerability, one that no one knows about and which has no patch from the vendor? That's a difficult problem, but Kaspersky Lab has a solution to help lower the risks: **Automatic Exploit Prevention** (AEP)[4] .

AEP is a comprehensive set of technologies that prevents exploits from using vulnerabilities in a wide range of programs and operating systems. Even if an exploit manages to launch, AEP can still prevent malicious behaviour from escalating. This technology is based on real-time behaviour analysis, as well as information on the applications that are most attacked by criminals – Adobe Acrobat, Java, Windows components, Internet Explorer and other popular software. Any time these programs attempt to launch suspicious code, safety controls immediately intervene, interrupt the launch and trigger a system scan while initiating Kaspersky's emergency system restore technology. **Independent test results**[5] repeatedly confirm that our AEP technology is a genuinely effective way of combating unknown and zero-day vulnerabilities.

[4] Source: http://eugene.kaspersky.com/2012/05/25/the-dangers-of-exploits-and-zero-days-and-their-prevention/
[5] Source: http://www.mrg-effitas.com/wp-content/uploads/2012/06/MRG-Effitas-Exploit-Prevention-Test1.pdf

Meet Your New Controller

One distinguishing feature of Icefog is the extent to which its operators interact with it manually. Usually, malware infections are designed to perform automated data exfiltration tasks. With Icefog, though, a human operator follows up each infection, connecting to the machine, personally identifying the victim and deploying tools to steal valuable data. The operator can deploy any other malicious tool having full access to the system, as if he was sitting at the desktop console. For example, he could install seemingly legitimate versions of remote control admin applications that an antivirus engine would not recognize as malware. If this happens, even after the initial Icefog code is detected, the attackers can maintain direct control of the infected machine(s).

Sophisticated attacks like this demand a sophisticated defense — the **Whitelist Security Approach**[6]. Only trusted applications are allowed to run and, moreover, a strict list of such trusted applications can be created while no other application is allowed to execute. This technology is called Default Deny. In this mode, workstations operate in an isolated software environment, where attacks like Icefog simply cannot be launched. It can't launch and hide its' remote software tools if they are not in the "allowed applications" list.

Icefog is a newly discovered threat that is increasingly active in cyberspace – but by exercising the right security approach and using the described technologies that are a part of **Kaspersky Endpoint**[7] **Security for Business** — you'll be fully protected.

[7] http://www.kaspersky.com/business-security/endpoint-advanced