GLOBAL CYBER SECURITY INCIDENCE REPORT

NEW MEDIA AND INFORMATION SECURITY DEPARTMENT

MAY 2015

1. 'Moose' malicious worm targets home routers

The "moose" malware tries to take over home routers by trying thousands of weak passwords.

Once it has taken over a device, the worm grabs login details when people visit Twitter, Facebook, Instagram, YouTube and other social sites.

These credentials are then used to artificially inflate followers and viewer numbers.

"This threat is all about social network fraud," said researchers Olivier Bilodeau and Thomas Dupuy from security firm Eset in a report detailing their findings.

The malicious program got its name because the file containing its attack code is called elan - French for moose.

The malicious worm travels the internet "aggressively" seeking out vulnerable devices. So far, said the pair, some of the routers made by Actiontec, Hik Vision, Netgear, Synology, TP-Link, ZyXEL, and Zhone have been found to be vulnerable to moose.

In their analysis, the two researchers saw the worm being used to set up bogus accounts on social network sites and then use stolen credentials to add fake "likes" and "follows" to those accounts.

Solutions:

- Always use strong passwords
- Use different passwords for all user accounts.
- Change passwords immediately if they may have been compromised.
- Encrypting password is also a strong protection method

http://www.bbc.com/news/technology-32915997

2. Android Ransomeware

Cybercrooks have launched a new wave of Android ransomware that poses as a pretty convincing FBI-imposed porn-surfing warning.

Over 15,000 spam emails, including zipped files, have hit the inboxes of Android users in recent days, according to Romanian security software firm Bitdefender.

If activated, the ransomware demands $500 to restore access. Users that try to independently unlock their devices will see the amount increase to $1,500, with payment demanded via Money Pak and PayPal My Cash transfers.

The malware poses as an Adobe Flash Player update, a common malware slinging ruse.
“After pressing 'OK' to continue, users see an FBI warning and cannot escape by navigating away,” states Catalin Cosoi, Chief Security Strategist at Bitdefender.

“The device’s home screen delivers an alarming fake message from the FBI telling users they have broken the law by visiting pornographic websites. To make the message more compelling, hackers add screenshots of the so-called browsing history. The warning gets scarier as it claims to have screenshots of the victims’ faces and know their location," said Cosoi.

MODE OF ATTACKS

The malware does not encrypt the contents of compromised smartphones, instead it renders the device’s home screen button and back functionalities inoperable.

"Turning the device on/off doesn’t help either, as the malware runs when the operating system boots,” according to Cosoi.

SOLUTIONS

If ADB (Android Data Bridge) is enabled on the infected Android, users can uninstall the offending application by starting to start the terminal in Safe Boot.
This option loads a minimal Android configuration and prevents the malware from running, which can buy enough time to manually uninstall the malware.

http://www.theregister.co.uk/2015/05/26/android_ransomware_mobile_scam_fbi/

3. Small-to Mid-sized Organizations Targeted By 'Grabit' Cyberspies

Researchers have discovered an aggressive attack campaign against SMBs around the globe that appears to be targeting the chemical, nanotechnology, education, agriculture, media, and construction sectors for intelligence purposes.

MODE OF ATTACKS

Kaspersky Lab researchers gave details about the newly discovered Grabit malware and its attack campaign that has been underway since February of this year and remains active. The cyber espionage attack has stolen some 10,000 files from victims mostly in Thailand, India, and the US; but Kaspersky has seen victims in the United Arab Emirates, Germany, Israel, Canada, France, Austria, Sri Lanka, Chile, and Belgium.

The attackers appear to be after everything from credentials to system information. "Based on the research, it stated that credentials is not the main focus and that Grabit collects internal information about the system – firewall, anti-virus installed, machine name, internal/external IPs, keylog, screenshots, machine time [and] language and more," says Ido Naor, senior security researcher for Kaspersky Lab's Global Research & Analysis Team.

The attack begins with a phishing email outfitted with a malicious Word document. Once the user opens the attachment, the malware is delivered to the user's machine via a remote legitimate server that hosts the malware, which is based on the infamous commercial HawkEye keylogger kit used for cyberspying. The attackers also deliver several remote administration tools, or RATs, to the victim.

Solutions

- Keeping antivirus up to date.
- Avoid opening unknown attachments.
- There are a few ways to check for Grabit infections, according to Kaspersky: the C:\Users\<PC-NAME>\AppData\Roaming\Microsoft area of a user's machine has executable files; or if the Windows System Configuration includes "grabit1.exe" in the startup table. "Run “msconfig” and ensure that it is clean from grabit1.exe records.

http://www.darkreading.com/endpoint/small-to-mid-sized-organizations-targeted-by-grabit-cyberspies/d/d-id/1320613