PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Threats and vulnerabilities

New zero-day exploit targets Adobe Flash Player

Phishing

Cybercriminals use new tricks in phishing attacks

Malware

Malware families attacking business networks continue to grow

Top story

Connected cars: The open road for hackers

pwc

New zero-day exploit targets Adobe Flash Player

The critical vulnerability affects Adobe Flash Player 21.0.0.242 and earlier versions for the following operation systems:

Windows
Mac OS X
Linux
Chrome OS

The zero-day (CVE-2016-4171) is due to be patched today (16 June) as part of Adobe's monthly security update.

Flash Player users are advised to immediately update to the latest version once it is available. Since this vulnerability is already being exploited in the wild, users should make updating this software a priority.

With the number zero-day exploits being discovered continuing to rise the efforts of hackers trying to profit from these types of attacks show no signs of letting up anytime soon.

According to findings in Symantec's 2016 Internet Security Threat Report zero-days rose by a staggering 125% last year, meaning a new vulnerability was discovered every week (on average). This just goes to highlight that zero-day attacks are now of the most common go to techniques that cyber-criminals are using in their malicious activities.

"Zero-day exploits are VERY profitable," Luis Corrons, PandaLabs Technical Director at Panda Security, told Infosecurity. "This is because during the window of time in which the vulnerability is being exploited and a patch is released, and then applied, anyone exposed to it will be compromised."

However, there are a number of security measures that can be taken to reduce the risk of being hit by zero-days such as never installing unnecessary software and making sure any software you do have is fully updated, Corrons said.

The best approach is to use security services that include anti-exploit technologies and that monitor all processes running in the computers, so as long as a trustable process starts behaving strangely, it can be noticed and blocked in time," he added.

Source:
http://www.infosecurity-magazine.com/news/new-zeroday-exploit-targets-adobe/

Cybercriminals use new tricks in phishing attacks

Researchers have observed phishing attacks where cybercriminals used some new tricks to avoid raising suspicion and make their operations more efficient.

An increasing number of cybercrime groups have come to realize that phishing attacks aimed at business executives can be highly profitable, but campaigns aimed at the masses can also be lucrative, which is why some malicious actors have been working on improving their methods.

Misconfigured temporary URLs

Earlier this month, Sucuri reported spotting an interesting technique used by attackers in phishing campaigns. Cybercriminals need to regularly change the domains that host their phishing pages to avoid getting blocked by security products and now they appear to have found a new way to obtain the domains they need.

According to researchers, attackers have been leveraging the fact that hosting providers, including some of the major ones, have failed to properly configure temporary URLs. These URLs, which look something like http://server-name/~username/, are offered to users in order to allow them to test their websites before linking them to their own domains.

When these temporary URLs are not configured properly, one user's files can be accessed through any domain name on the same server. An attacker can register an account on a shared server, upload their phishing pages, and compile a list of other sites on that server.

If the temporary URLs are not set up properly, the phishing pages will be accessible from any of the neighboring domain names. For example, if the attacker uploads the phishing page to/~attacker/phishing on their own site, the page will also be accessible from neighbor-site1.xyz/~attacker/phishing, neighbor-site2.xyz/~attacker/phishing, etc

.

"As a result, one server account gives them hundreds of different domains for their malicious pages for free. They can frequently change the domains without disclosing the real location of the malicious files and without having to move their files to different places when the domains get blacklisted," Sucuri researcher Denis Sinegubko explained in a blog post.

The technique has been spotted in the wild and the security firm has observed instances where a legitimate website had been blacklisted because it was hosted on the same server as a malicious site.

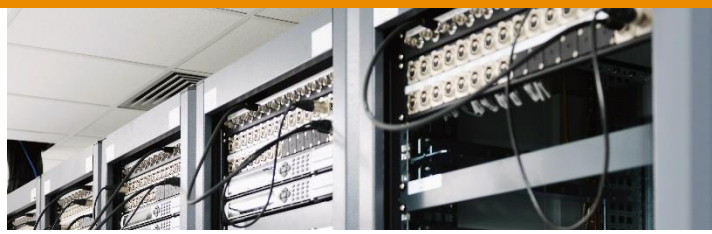
Website owners can check if they are affected by trying to access their sites using their own domain name (e.g. http://your-domain.com/~yourusername). If it works, the hosting provider has not configured temporary URLs properly.

Using JavaScript to silently steal credentials

A UK-based researcher who uses the online moniker dvk01uk reported coming across a PayPal phishing email that leveraged a clever technique to trick recipients into thinking that the details they provided were sent to the payment processor's servers

Source:
http://www.securityweek.com/cybercriminals-use-new-tricks-phishing-attacks

Malware families attacking business networks continue to grow



The number of active global malware families increased by 15 percent in May 2016, according to Check Point. They detected 2,300 unique and active malware families attacking business networks in May. The continued rise in the number of active malware variants highlights the wide range of threats and scale of challenges security teams face in preventing an attack on their business critical information.

While Conficker remained the most commonly used malware in the period, banking malware Trojan Tinba became the second most prevalent form of infection last month, allowing hackers to steal victim's credentials using web-injects, activated as users try to log-in to their banking website.

Attacks against mobile devices also remained constant as Android malware HummingBad remained in the overall top 10 of malware attacks across all platforms globally during the period. Despite only being discovered by Check Point researchers in February, it has rapidly become commonly used; indicating hackers view Android mobile devices as weak spots in enterprise security and as potentially high reward targets.

"We continue to see a significant increase in the number of unique and active malware families targeting business networks, which speaks to the effort hackers are putting into creating new zero-day attacks and the scale of the challenge businesses face in securing their network against cyber criminals," said Nathan Shuchami, head of threat prevention, Check Point. "Organizations need to consider using advanced threat prevention measures on networks, endpoints and mobile devices to stop malware at the pre-infection stage to ensure they are effectively secured against the latest threats."

In May, Conficker was the most prominent family accounting for 14 percent of recognized attacks; while second and third placed Tinba and Sality were responsible for 9 percent each. The top ten families were responsible for 60 percent of all recognized attacks.

1. **Conficker** – Worm that allows remote operations, malware downloads, and credential theft by disabling Microsoft Windows systems security services. Infected machines are controlled by a botnet, which contacts its Command & Control server to receive instructions.

2. **Tinba** – Also referred to as Tiny Banker or Zusy, Tinba is a banking trojan that steals the victim's credentials using web injections. It becomes activated when users try to login to their banking website.

3. **Sality** – Virus that infects Microsoft Windows systems to allow remote operations and downloads of additional malware. Due to its complexity and ability to adapt, Sality is widely considered to be one of the most formidable malware to date.

Mobile malware families continued to pose a significant threat to businesses mobile devices during May with six entries into the top 100 overall families. Most of these targeted Android, but in a continuation of the trend seen in April several targeted iOS. The top three mobile families were:

4. **HummingBad** – Android malware that establishes a persistent rootkit on the device, installs fraudulent applications, and with slight modifications could enable additional malicious activity such as installing a keylogger, stealing credentials and bypassing encrypted email containers used by enterprises.

Source:
https://www.helpnetsecurity.com/2016/06/21/malware-families-attacking-business-networks-grows/

Connected cars: The open road for hackers

Car hacking?

Vehicles have come a long way in terms of the high-tech features and connectivity that come standard in most new models. Modern cars are controlled almost entirely by software, and many drivers don't realize the most complex digital device they own may be in their driveway. Of the growing number of devices in the "Internet of Things" (IoT), vehicles are among the most significant additions to the global Internet. An ever-growing list of features—including web browsing, Wi-Fi access points, and remote-start mobile phone apps—enhance user enjoyment, but also greatly expand vehicles' attack surface, rendering them potentially vulnerable to advanced attacks. During the past year especially, numerous proof-of-concept demonstrations have revealed connected-car vulnerabilities that malicious actors can exploit, ranging from unauthorized entry to commandeering the vehicle's operation. Unfortunately, as consumer demand drives ever more features, the opportunities for compromise will increase as well.

Ransomware

The scourge of ransomware has so far affected thousands of systems belonging to ordinary individuals, hospitals, and police stations. A vehicle's increased connectivity, ever-expanding attack surface, and high upfront cost make them attractive ransomware targets. In contrast to ransomware that infects ordinary computer systems, vehicles are more likely susceptible to ransomware attacks when their disablement causes knock-on effects.For example, where a single driver might be able to reinstall his car's software with the help of a mechanic to remedy a ransomware infection, a group of vehicles disabled on a busy highway could cause far more serious disruption. Victims or municipal authorities may have little choice but to pay the ransom to reopen a busy commuting route. Alternatively, a logistics company might suddenly find a large portion of its truck fleet rendered useless by ransomware. The potential for lost revenue due to downtime might pressure the company to pay the ransom rather than risk more significant financial losses.

Malicious C2 and Final Hop Points

One effective law enforcement tactic in countering cyber espionage and criminal campaigns is identifying, locating and seizing the systems threat actors use to route malicious traffic through the Internet. Since many modern vehicles can be better described as a computer attached to four wheels and an engine, their mobility and power present challenges to this means of countering threat activity. We have already witnessed malware designed to hijack IoT devices for malicious purposes; vehicular systems' greater computing power, compared to connected home thermostats, can significantly enhance their value as a C2 node.

Source:
https://www.fireeye.com/blog/threat-research/2016/06/connectedcarsthe.html

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

MB/June 6655