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.

Malware

GoldenEye ransomware targets HR departments with fake job applications

Threats and vulnerabilities

Critical zero-day flaws found in PHP 7: One remains unpatched!

Threats and vulnerabilities

Critical PHPMailer flaw leaves millions of websites vulnerable to remote exploit

Top story

NIST guide provides way to tackle cybersecurity incidents with recovery plan, playbook

pwc

GoldenEye ransomware targets HR departments with fake job applications

A variant of the Petya ransomware dubbed GoldenEye is targeting human resources (HR) with fake job applications infected with malware.

GoldenEye has been around for some time, but security firm Check Point notes that it has recently turned its attention to HR staffers that frequently open emails from unknown sources.

The campaign, which is targeting HR employees in Germany, lures victims in with a legitimate looking job application. There are two files attached to the email: a PDF containing a cover letter which has no malicious content and its primary purpose is to lull the victim into a false sense of security, and an Excel file with malicious macros unbeknown to the receiver.

The latter contains a picture of a flower with the word "Loading..." underneath, and a text in German asking the victim to enable content so that the macros can run.

"When a user clicks "Enable Content", the code inside the macro executes and initiates the process of encrypting the files, denying the victim access to his or her files," Check Point explains.

"GoldenEye then, appends a random 8-character extension to each encrypted file. After all the files are encrypted, GoldenEye presents the ransom note: "YOUR_FILES_ARE_ENCRYPTED.TXT" After displaying the ransom note, GoldenEye forces a reboot and starts encrypting the disk.

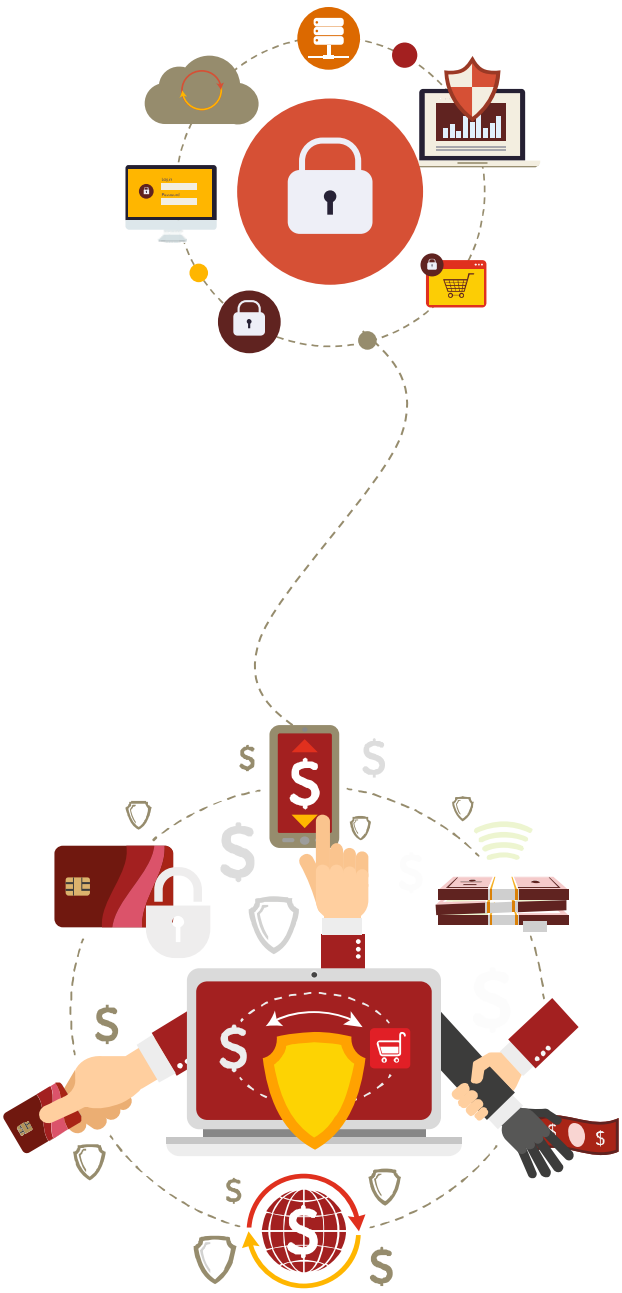
"This action makes it impossible to access any files on the hard disk. While the disk undergoes encryption, the victim sees a fake "chkdsk" screen, as in previous Petya variants."

From here, users are presented with a ransom note - the same seen in previous Petya campaigns but with a new gold colour scheme (*above*). The victim is presented with a "personal decryption code", which can enter be in a Dark Web portal in order to pay the ransom.

The current ransom demanded by GoldenEye begins at 1.3 BitCoins (BTC), which works out at approximately $1,000 (around £810).

Source:

http://www.theinquirer.net/inquirer/news/3001887/goldeneye-ransomware-targets-hr-departments-with-fake-job-applications



Critical zero-day flaws found in PHP 7: One remains unpatched!

Three critical zero-day vulnerabilities have been discovered in PHP 7 that could allow an attacker to take complete control over 80 percent of websites which run on the latest version of the popular web programming language.

The critical vulnerabilities reside in the un serialized mechanism in PHP 7 – the same mechanism that was found to be vulnerable in PHP 5 as well, allowing hackers to compromise Drupal, Joomla, Magento, vBulletin and websites and other web servers in the past years by sending maliciously crafted data in client cookies.

Security researchers at Check Point's exploit research team spent several months examining the unserialized mechanism in PHP 7 and discovered "three fresh and previously unknown vulnerabilities" in the mechanism.

While researchers discovered flaws in the same mechanism, the vulnerabilities in PHP 7 are different from what was found in PHP 5.

Tracked as CVE-2016-7479, CVE-2016-7480, and CVE-2016-7478, the zero-day flaws can be exploited in a similar manner as a separate vulnerability (CVE-2015-6832) detailed in Check Point's August report.

- CVE-2016-7479—Use-After-Free Code Execution
- CVE-2016-7480—Use of Uninitialized Value Code Execution
- CVE-2016-7478—Remote Denial of Service

The first two vulnerabilities, if exploited, would allow a hacker to take full control over the target server, enabling the attacker to do anything from spreading malware to steal customer data or to defacing it.
The third vulnerability could be exploited to generate a Denial of Service (DoS) attack, allowing a hacker to hang the website, exhaust its memory consumption and eventually shut down the target system, researchers explain in their report [PDF].

According to Yannay Livneh of Check Point's exploit research team, none of the above vulnerabilities were found exploited in the wild by hackers.
The check Point researchers reported all the three zero-day vulnerabilities to the PHP security team on September 15 and August 6. Patches for two of the three flaws were issued by the PHP security team on 13th October and 1st December, but one of them remains unpatched.

Besides patches, Check Point also released IPS signatures for the three vulnerabilities on the 18th and 31st of October to protect users against any attack that exploits these vulnerabilities.
In order to ensure the webserver's security, users are strongly recommended to upgrade their servers to the latest version of PHP.

Source:
http://thehackernews.com/2016/12/php-7-update.html

Our perspective

Critical vulnerabilities have been reported by researchers which, if exploited successfully by cybercriminals, will lead to major security breaches. Web server administrators are advised to assess the risk and vulnerabilities in their specific environment and upgrade to the latest available version of PHP.

Critical PHPMailer flaw leaves millions of websites vulnerable to remote exploit

A critical vulnerability has been discovered in PHPMailer, which is one of the most popular open source PHP libraries to send emails used by more than 9 Million users worldwide.

Millions of PHP websites and popular open source web applications, including WordPress, Drupal, 1CRM, SugarCRM, Yii, and Joomla comes with PHPMailer library for sending emails using a variety of methods, including SMTP to their users.

Discovered by Polish security researcher Dawid Golunski of Legal Hackers, the critical vulnerability (*CVE-2016-10033*) allows an attacker to remotely execute arbitrary code in the context of the web server and compromise the target web application.

"To exploit the vulnerability an attacker could target common website components such as contact/feedback forms, registration forms, password email resets and others that send out emails with the help of a vulnerable version of the PHPMailer class," Golunski writes in the advisory published today.

Golunski responsibly reported the vulnerability to the developers, who have patched the vulnerability in their new release, PHPMailer 5.2.18.

All versions of PHPMailer before the critical release of PHPMailer 5.2.18 are affected, so web administrators and developers are strongly recommended to update to the patched release.

Since The Hacker News is making the first public disclosure of the vulnerability in the news following Golunski advisory and millions of websites remain unpatched, the researcher has put on hold more technical details about the flaw.

However, Golunski has promised to release more technical details about the vulnerability in coming days, including a proof-of-concept exploit code and video demonstration that will show the attack in action.

We will update this article with additional information on the PHPMailer vulnerability, exploit code and video demonstration, once the researcher makes it public.

Golunski has released Proof-of-Concept (PoC) exploit code for PHPMailer remote code execution vulnerability.

"A successful exploitation could let remote attackers gain access to the target server in the context of the web server account which could lead to a full compromise of the web application," Golunski said.

You can find exploit code here.

Source:
http://thehackernews.com/2016/12/phpmailer-security.html

NIST guide provides way to tackle cybersecurity incidents with recovery plan, playbook

"Defense! Defense!" may be the rallying cry from cybersecurity teams working to thwart cybersecurity attacks, but perhaps they should be shouting "Recover! Recover!" instead. Attackers are increasingly racking up points against their targets, so the National Institute of Standards and Technology (NIST) has published the *Guide for Cybersecurity Event Recovery* to help organizations develop a game plan to contain the opponent and get back on the field quickly.

As the number of cybersecurity incidents climbs, and the variety of types of attacks grows, "It's no longer if you are going to have a cybersecurity event, it is when," said computer scientist Murugiah Souppaya, one of the guide's authors.

For example, the number of companies experiencing ransomware events, in which attackers hold an organization's data hostage until the ransom is paid, have tripled between the first and third quarters of 2016 alone, according to the December 2016 *Kaspersky Security Bulletin* .

In addition to the overall rise in incidents, the 2015 Cybersecurity Strategy and Information Plan(link is external)(CSIP), published by the Office of Management and Budget, identified inconsistent cybersecurity response capabilities across the federal government and called for agencies to improve these skills.

The CSIP defines "recover" as developing and implementing plans, processes and procedures to fully restore a system weakened during a cybersecurity event. Recovering may be as simple as restoring data from a backup, but usually it is more involved and the system may be brought back online in stages.

Recovery is a critical piece of the risk management process. Yet no federal policies, standards or guidelines focus specifically on recovering from a cybersecurity incident. And prior to the new report, no one publication has addressed recovery approaches in one place.

NIST guide provides way to tackle cybersecurity incidents with recovery plan, playbook

NIST computer researchers wrote the *Guide for Cybersecurity Event Recovery* to consolidate existing NIST recovery guidance such as on incident handling and contingency planning. It also provides a process that each organization—federal or otherwise—can use to create its own comprehensive recovery plan to be ready when a cybersecurity event occurs.

The publication supplies tactical and strategic guidance for developing, testing and improving recovery plans, and calls for organizations to create a specific playbook for each possible cybersecurity incident. The guide provides examples of playbooks to handle data breaches and ransomware.

This document also provides additional information related to the "Recover" function in the *Framework for Improving Critical Infrastructure Cybersecurity*, more commonly known as the Cybersecurity Framework.

"To be successful, each organization needs to develop its own plan and playbooks in advance," said Souppaya. "Then they should run the plays with tabletop exercises, work within their team to understand its level of preparation and repeat."

Source:
https://www.nist.gov/news-events/news/2016/12/nist-guide-provides-way-tackle-cybersecurity-incidents-recovery-plan

Our perspective

From the Swift hack to the DNC hack, every year, security breach events have continued to increase, exploiting weaknesses in processes, people and technologies. We believe that focusing entirely on preventing cyber events is a partial approach. Organisations should also improve their prevention capabilities by adopting modern technology and tools while augmenting their cyber event detection and response capabilities. It is also important for organisations to improve resilience by ensuring that their risk management processes include comprehensive recovery planning. NIST has been very active in designing and modifying the Cybersecurity Framework (CSF), which consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritised, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cyber security-related risks. The NIST Guide for Recovery (NIST Special Publication 800-184) provides guidance to help organisations plan and prepare for recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.

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 2,23,000 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. 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/January2017-8363