Check Point
SOFTWARE TECHNOLOGIES LTD.

May 11 - 17, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Supercomputers in Switzerland, Germany and the UK have been infected by what looks like a cryptocurrency mining malware. Some of the supercomputers were being used to research COVID-19, and are still down for forensic investigation. The attackers appear to have gained access to the supercomputer clusters via compromised SSH credentials.
- UK's ministry of defense contractor "Interserve", support services and construction company, has suffered a data breach. Attackers have stolen up to 100,000 past and present employees' personal details including payment and payroll information.
- Researchers have uncovered a new Trojan dubbed QNodeService, used in a Coronavirus-themed phishing campaign. The operators behind the campaign promise COVID-19 tax relief, to lure victims to run the malicious file.

  Check Point Anti-Virus product provides protection against this threat (backdoor.Win32.qnode)
- Diebold Nixdorf, major ATM manufacturer, has suffered a ransomware attack that caused only "a limited IT systems outage." The company discloses the security breach but pointed out that the infection did not impact its ATMs or customer networks.

  Check Point SandBlast provides protection against this threat
- Magellan Health, a US healthcare company, has been hit by ransomware. The attack took place on April 11, 2020, and included a data breach of personal information from one of the corporate servers.

  Check Point SandBlast provides protection against this threat
- REvil ransomware, which has recently breached celebrity law firm Grubman Shire Meiselas & Sacks, has increased the ransom demand to $42M. In parallel, the hackers have started releasing leaked client emails, some of them mentioning US President Donald Trump.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.REvil)

VULNERABILITIES AND PATCHES

- Researchers have uncovered a set of 7 new unpatchable hardware vulnerabilities that affect all desktops and laptops sold in the past 9 years with Thunderbolt, or Thunderbolt-compatible USB-C ports. Exploitation of these vulnerabilities cannot be done remotely, and would require physical access to the computer.
- Microsoft has released its March 2020 Patch Tuesday security updates to fix 111 vulnerabilities. 16 are rated critical while the rest have been ranked important.

  Check Point IPS provides protection against these threats

- A critical vulnerability in the WP Product Review life, WordPress plugin that helps site owners create custom review articles using pre-defined templates and installed on over 40,000 sites, can lead to malicious code injection and potentially taking-over vulnerable websites.

THREAT INTELLIGENCE REPORTS

- Check Point Research, analyzing Microsoft's patch for CVE-2020-0655, have found that the patch added a workaround to fix the vulnerability, but does not address the core vulnerability in the PathCchCanonicalize function. The vulnerability can still be exploited to modify and steal data, among other attacks.
- Check Point Research have discovered new phishing campaigns impersonating the WHO and popular conferencing platforms, to steal sensitive information. Check Point has seen 192,000 coronavirus-related cyber-attacks per week over the past three weeks, a 30% increase compared to previous weeks.
- The US government has released information on three new malware variants used in malicious cyber activity campaigns by a North Korean government-backed hacker group tracked as HIDDEN COBRA.

  Check Point SandBlast, Anti-Bot and Anti-Virus provide protection against this threat (Generic.Win32.HiddenCobra)

- Edison, iPhone Email application, has released a version that contained a bug that caused accounts and massages to sync on devices used by other people. Edison responded by reverting the update and informing that only a "small percent" of users were affected.
- Researches have exposed a new cyberespionage campaign carried out by the Russia-linked APT group Turla, using a new version of the COMpfun malware. The new variant allows attackers to control hosts using a HTTP status codes.

  Check Point SandBlast and Anti-Bot provide protection against this threat

For comments, please contact: TI-bulletin@checkpoint.com