November 12-18, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers found that the Hades APT group, responsible for the infamous Olympic Destroyer attack during the 2018 Winter Olympic Games, has been carrying out a new wave of attacks in which more complex macros and a new dropper variant were distributed.
- Vision Direct, a European online supplier for contact lens, has been breached. Customer data has been compromised, including name, billing and email addresses, password, credit card number and CVV.
- A massive phishing campaign has been hitting banking users in Russia. The fraudulent emails pretend to originate from Central Bank of Russia, luring recipients to open the malicious attachment.
- tRat, a new modular malware, has been distributed by the TA505 APT group in a campaign using Word documents with malicious macros abusing the Norton Security brand, and by another campaign targeting commercial banking institutions.
- The infamous tech support scam has taken on a new form, leveraging the Facebook Sharer dialogue, a page typically used by website owners to invite users to share their content. A warning is urging users to call the regional Facebook support team, who will then connect to the victim's computer remotely, install malware and/or try to sell them unnecessary products/services.
- City of York Council has reported the personal details of users of its mobile app, One Planet York, have been compromised. It is yet unclear if the details were gained by attacking end-users through the app, or by accessing York's database.
- A new variant of the notorious TrickBot banking Trojan has been targeting the British Lloyds Bank clients. The malicious emails impersonate the bank's email address to lure users to open malicious attachments. The installed malware would then try to steal banking credentials and additional data form the infected computer.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Trickbot)

VULNERABILITIES AND PATCHES

- Siemens AG issued fixes for eight vulnerabilities in its industrial product lines. Among them is a patch for a cross-site scripting vulnerability in Siemens' SCALANCE firewall product. The flaw could allow an attacker to gain access to industrial networks.
- Attackers have been exploiting a bug in a popular GDPR compliance plugin for WordPress to gain control over vulnerable websites. The plugin developer, WP GDPR Compliance, has issued a patch for the bug.

  Check Point IPS blade provides protection against all known variants of this threat (WordPress GDPR Compliance Plugin Privilege Escalation)
- An information leakage vulnerability in the Android mobile operating system may allow an attacker close to a Wi-Fi router to track the location of Android users located within the router's range.
- The popular smart wristwatch for kids, 'Kids Watcher', has been found to contain a set of flaws that could enable an attacker to collect real-time GPS coordinates, personal credentials and even eavesdrop on conversations.
- Researchers have uncovered a bug in Gmail that can be exploited to place emails in a user's Sent folder, even if they weren't sent by the user at all, as well as in to force the email into the Inbox. Usage of this flaw may help attackers make sure their phishing emails don't arrive to the Spam folder.

THREAT INTELLIGENCE REPORTS

- In preparations for the upcoming Black Friday, researchers have issued a review of the most prominent threats targeting e-commerce users. Top targeted websites are 'consumer apparel' portals, and top targeted countries are Italy, Germany and France.
- Cybercriminals are expected to use artificial intelligence to significantly speed the process of detecting zero-day vulnerabilities, according to a research reviewing the techniques that would be used by attackers in the future.
- An article is reviewing the dangers that lie in expired domains – domains whose owners did not pay the renewal fee on time. Such domains have recently been widely used by attackers, who gain control over the website as soon as they expire and distribute malware to the website customers.
- Researchers have analyzed Emotet, a botnet and banking Trojan first observed in 2014. The research concluded that the banker uses two attack infrastructures in parallel, will be followed by details about the possible origins of the person behind the botnet.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.Emotet)