Weekly Comments

18 - 25 September 2018

MageCart skimmer attacks continue to be in the limelight this week. Online tech retailer Newegg and ABS-CBN, one of the largest media and entertainment groups in the Philippines, are the latest MageCart victims after attackers injected the skimmer on their websites to pilfer credit card details. Further investigation shows that the Newegg attack had used a skimmer script smaller than that in the British Airways attack–this confirms earlier suspicions that the attackers are constantly honing their craft to minimise detection. The success of these high-profile attacks will likely boost the confidence of the attackers. And as some researchers surmise, the attackers are expected to continue targeting prominent brands and perform highly targeted attacks with further condensed scripts to minimise detection.

Meanwhile, Adobe has issued out-of-band security updates to address several vulnerabilities in its Acrobat Reader and Document Cloud products. The most critical vulnerability (CVE-2018-12848) is an out-of-bounds write vulnerability that could lead to arbitrary code execution. Other important vulnerabilities (CV3-2018-12801, CVE-2018-12840, CVE-2018-12849, CVE-2018-12850, CVE-2018-12775, CVE-2018-12778) are out-of-bounds read vulnerabilities that could lead to information disclosure. The vulnerabilities have not been exploited in the wild.

Trend Micro's Zero Day Initiative (ZDI) team has also publicly disclosed a serious remote code execution vulnerability in the Microsoft JET Database engine used by several Microsoft products. There is currently no patch for the vulnerability. An attacker could exploit this vulnerability to execute code under the context of the current process, but it requires user interaction as the target has to open a malicious file containing data stored in the JET database format. Various applications use this database format. In the absence of a patch, we urge users to stay vigilant and refrain from opening files from untrusted sources.

References:

[1] Another Victim of the Magecart Assault Emerges: Newegg

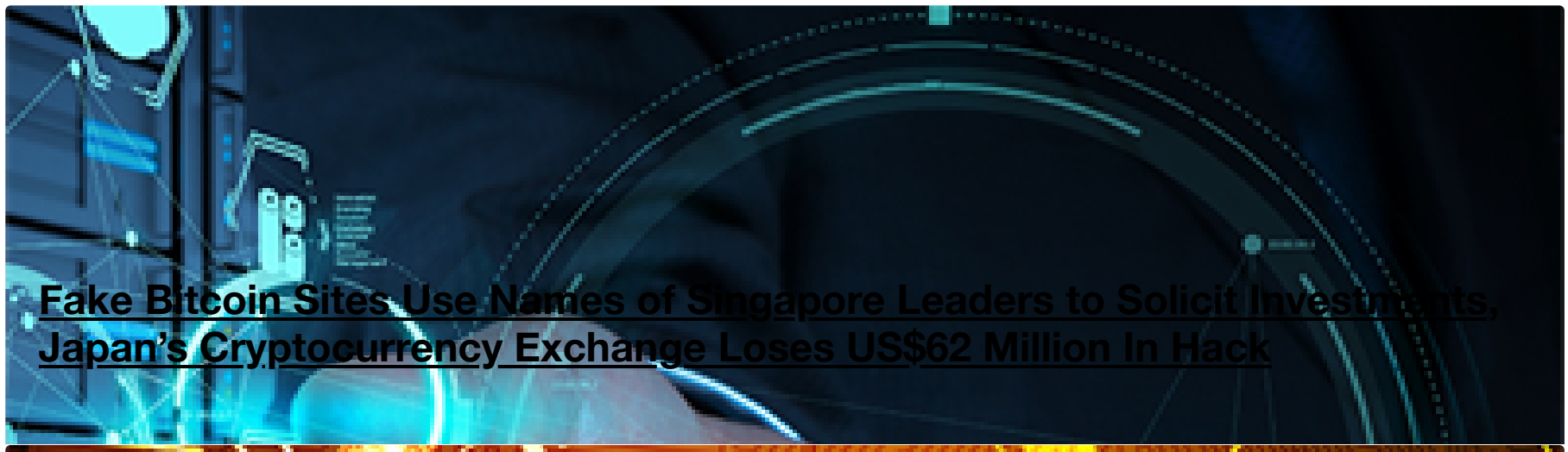
More Weekly Cyber News

Financial Aid Office of U.S. Department of Education Hit By Phishing Attack

ABS-CBN Sites Compromised By MageCart Skimmer, China Arrests Suspect For Huazhu Group Data Breach

KrisFlyer Air Miles Sold in Dark Web Marketplaces, Chinese Police Arrest 21 Over Data Theft at Alibaba's Delivery Arm

Suspected Pegasus Spyware Infection Found in Singapore, ICA Warns of Fake Visa Application Site



Fake Bitcoin Sites Use Names of Singapore Leaders to Solicit Investments, Japan's Cryptocurrency Exchange Loses US$62 Million In Hack

SingHealth Cyber Attacker Entered Network In August Last Year, TheDarkOverLord Resurfaces With Stolen Patient Records

Weekly Comments

18 - 25 September 2018

MageCart skimmer attacks continue to be in the limelight this week. Online tech retailer Newegg and ABS-CBN, one of the largest media and entertainment groups in the Philippines, are the latest MageCart victims after attackers injected the skimmer on their websites to pilfer credit card details. Further investigation shows that the Newegg attack had used a skimmer script smaller than that in the British Airways attack–this confirms earlier suspicions that the attackers are constantly honing their craft to minimise detection. The success of these high-profile attacks will likely boost the confidence of the attackers. And as some researchers surmise, the attackers are expected to continue targeting prominent brands and perform highly targeted attacks with further condensed scripts to minimise detection.

Meanwhile, Adobe has issued out-of-band security updates to address several vulnerabilities in its Acrobat Reader and Document Cloud products. The most critical vulnerability (CVE-2018-12848) is an out-of-bounds write vulnerability that could lead to arbitrary code execution. Other important vulnerabilities (CV3-2018-12801, CVE-2018-12840, CVE-2018-12849, CVE-2018-12850, CVE-2018-12775, CVE-2018-12778) are out-of-bounds read vulnerabilities that could lead to information disclosure. The vulnerabilities have not been exploited in the wild.

Trend Micro's Zero Day Initiative (ZDI) team has also publicly disclosed a serious remote code execution vulnerability in the Microsoft JET Database engine used by several Microsoft products. There is currently no patch for the vulnerability. An attacker could exploit this vulnerability to execute code under the context of the current process, but it requires user interaction as the target has to open a malicious file containing data stored in the JET database format. Various applications use this database format. In the absence of a patch, we urge users to stay vigilant and refrain from opening files from untrusted sources.

References:

[1] Another Victim of the Magecart Assault Emerges: Newegg
[2] [SingCERT] Alert on Critical Out-Of-Band Adobe Acrobat Vulnerability (CVE-2018-12848)
[3] ZDI-CAN-6135: A remote code execution vulnerability in the Microsoft Windows JET Database Engine

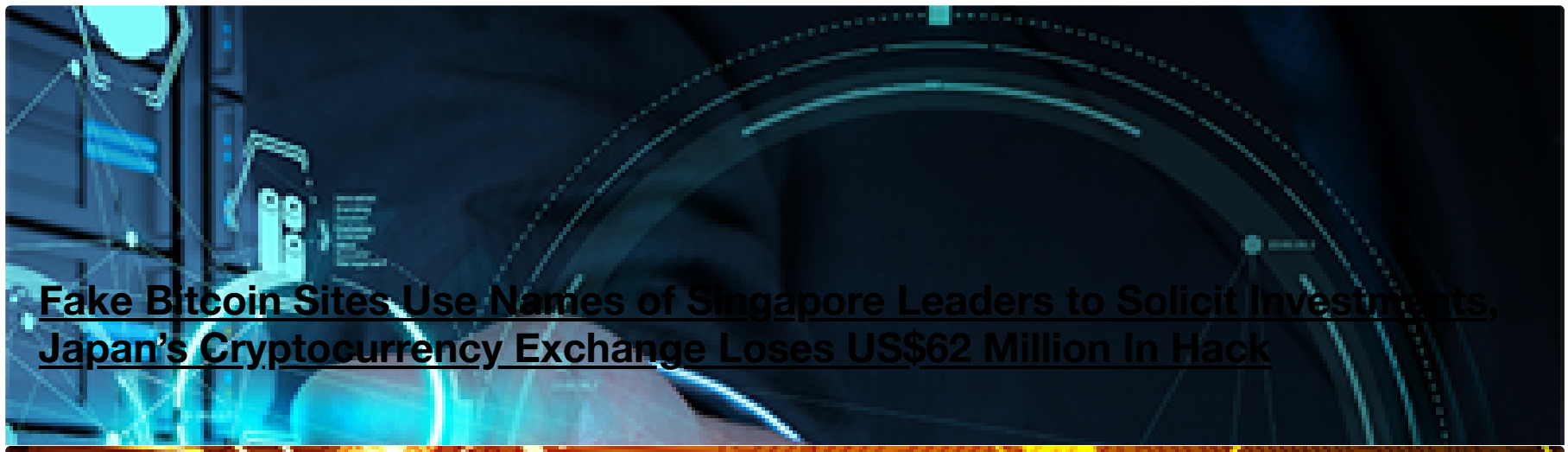
More Weekly Cyber News

Financial Aid Office of U.S. Department of Education Hit By Phishing Attack

ABS-CBN Sites Compromised By MageCart Skimmer, China Arrests Suspect For Huazhu Group Data Breach

KrisFlyer Air Miles Sold in Dark Web Marketplaces, Chinese Police Arrest 21 Over Data Theft at Alibaba's Delivery Arm

Suspected Pegasus Spyware Infection Found in Singapore, ICA Warns of Fake Visa Application Site



Fake Bitcoin Sites Use Names of Singapore Leaders to Solicit Investments, Japan's Cryptocurrency Exchange Loses US$62 Million In Hack

SingHealth Cyber Attacker Entered Network In August Last Year, TheDarkOverLord Resurfaces With Stolen Patient Records

Need cyber strategy consult, a proof-of-concept, or just some information?

Our domain experts are ready to tailor fit our proficiency to fit your cyber needs.

Contact Us

About Ensign InfoSecurity

As Southeast Asia's largest cybersecurity provider we are here to keep the region ahead of the game.

Follow us

Services

Ensign Consulting

Ensign Systems Integration

Ensign Managed Security Services

Ensign Labs

About Ensign

Awards & Accolades

News Room

Careers

The Ensign Difference

Cyber Insights

Analysis & Insights

Events

Join our Ensign Mailing List

Contact Us

Singapore

Malaysia

Hong Kong

South Korea