National Cybersecurity and Communications Integration Center

U.S. Secret Service

10 July, 2014

Keylogger Malware Found in Hotel Business Centers

This advisory was prepared in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC) and the United States Secret Service (USSS).

Executive Summary

As data breaches continue to result in devastating consequences for individual victims and often high reputational and financial risk for the entities that were breached, it's important to understand the balance of risk and convenience that your organization has chosen.[1,2] Analysis from companies like Symantec, Trustwave and Verizon all reveal that data breaches have increased at an alarming rate since at least 2011.[3,4,5] Unfortunately many of the reports state that malicious actors have targeted the Hospitality subsector over most others in that time frame.

The following is an advisory for owners, managers and stakeholders in the hospitality industry, which highlights recent data breaches uncovered by the United States Secret Service (USSS). The attacks were not sophisticated, requiring little technical skill, and did not involve the exploit of vulnerabilities in browsers, operating systems or other software. The malicious actors were able to utilize a low-cost, high impact strategy to access a physical system, stealing sensitive data from hotels and subsequently their guest's information. The NCCIC and the USSS have provided some recommendations at the end of this document that may help prevent similar attacks on publicly available computers.

Threat

The USSS North Texas Electronic Crimes Task Force recently arrested suspects who have compromised computers within several major hotel business centers in the Dallas/Fort areas. In some cases, the suspects used stolen credit cards to register as guests of the hotels; the actors would then access publicly available computers in the hotel business center, log into their Gmail accounts and execute malicious key logging software. The keylogger malware[6] captured the keys struck by other hotel guests that used the business center computers, subsequently sending the information via email to the malicious actors' email accounts. The suspects were able to obtain large amounts of information including other guests personally identifiable information (PII), log in credentials to bank, retirement and personal webmail accounts, as well as other sensitive data flowing through the business center's computers.

The USSS recommends that hotels in the area be on alert and take immediate action to determine if their business center computers have been infected by similar malware and to conduct a risk assessment of their publicly accessible machines. Although these specific breaches occurred outside of the hotel's enterprise system and the malicious activity was contained to stand-alone computers with segmented internet access, this type of exposure to patron data can result in significant impacts to consumer confidence, brand reputation and in some cases legal or financial liabilities.[7] This particular type of criminal activity highlights the importance of the need for physical and network security to work together as they are dependent on each other. Physical events can have cyber (logical data flow) consequences and cyber events can have physical consequences. As a dual mission agency, the

United States Secret Service has long recognized the importance of this methodology in its Protective mission of protecting people and events The USSS Critical System Protection methodology focuses on both the physical and local (cyber) assessment of events and has recognized that to be truly effective in protecting any system, you must establish, monitor and maintain control over both the physical and logical access of your assets.

Recommendations

The NCCIC and the USSS North Texas Electronic Crimes Task Force recommend that hotel managers, owners and other hospitality industry stakeholders consider the following.

Contacting your network administrator to request that:

- A banner be displayed to users when logging onto business center computers; this should include warnings that highlight the risks of using publicly accessible machines.[8]
- Individual unique log on credentials be generated for access to both business center computers and Wi-Fi;[9] this may deter individuals who are not guests from logging in.
- All accounts be given least privilege accesses; for example, guests logging in with the supplied user ID and password should not be able to download, install, uninstall, or save files whereas one authorized employee may have a need for those privileges to carry out daily duties. [10]
- Virtual local area networks (VLANs) are made available for all users, which will inhibit attackers from using their computer to imitate the hotel's main server.[11]
- All new devices are scanned (e.g. USB drives and other removable media) before they are attached to the computer and network[12]; disabling the Auto run feature will also prevent removable media from opening automatically.[13]
- Predetermined time limits are established for active and non-active guest and employee sessions.[14]
- Safe defaults are selected in the browsers available on the business center desktops (e.g. Internet Explorer, Mozilla Firefox). Options such as private browsing and 'do not track' for passwords and websites are some of the many available.[15]

Contact Information:

Any questions regarding this advisory can be directed to the United States Secret Service North Texas Electronic Crimes Task Force at (972) 868-3200 or email us at Dallas.ECTF@usss.dhs.gov. To be added to the normal distribution for similar products, please send requests to NCCIC@hq.dhs.gov or (888) 282-0870.

References:

[1] http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf
[2] http://www.experian.com/data-breach/data-breach-security.html
[3] http://www.symantec.com/connect/blogs/2013-internet-security-threat-report-year-mega-data-breach
[4] http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf
[5] http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-hospitality-threat-landscape_en_xg.pdf
[6] http://blog.kaspersky.com/keylogger/
[7] http://www.hospitalitylaboremploymentlawblog.com/2013/10/articles/employment-training-practices-and-procedures/effective-risk-management-of-growing-cyber-security-risk-in-the-hospitality-industry-2/
[8] http://prajwaldesai.com/how-to-configure-legal-notices-on-domain-computers-using-group-policy/
[9] http://msdn.microsoft.com/en-us/library/cc759279(v=ws.10).aspx
[10] http://www.sevenforums.com/system-security/251005-how-prevent-guest-account-making-modifications-computer.html
[11] https://www.hotelschool cornell.edu/research/chr/pubs/reports/abstract-14928.html
[12] http://www.staysafeonline.org/business-safe-online/protect-your-customers
[13] http://www.us-cert.gov/ncas/tips/ST08-001
[14] http://windows.microsoft.com/en-us/windows/control-when-children-use-computer#1TC=windows-7
[15] http://www.us-cert.gov/publications/securing-your-web-browser