The Vulnerabilities and Privileges of Carbanak Bank Thieves

February 17, 2015

Recently Kaspersky released analysis of a series of significant breaches against financial institutions by a group they have dubbed Carbanak. The attacks go back over 2 years and estimates are that potentially $1 billion dollars in total were stolen from more than 100 financial institutions. In some cases the attackers were active in victim organizations between two to four months. This allowed the attackers to specifically learn the internal workings of a target environment to then pivot and impersonate existing users to take control of money processing services, ATMs, SWITCH and even direct manipulation of databases in order to in the end extract money from these organizations. Within the Kaspersky analysis we can learn a good deal of how the attackers initially compromised systems, implanted malware, and moved laterally through the environment. We are highlighting here some of the ways in which proper vulnerability and privilege management would have helped mitigate certain aspects of these threats. There are a few documented vulnerabilities and techniques which the attacker leveraged for their initial point of entry. The two most common types of attacks appear to be spear phishing and drive-by web attacks. In the case of the spear phishing attacks the attackers emailed victims malicious Microsoft Office documents which exploited a few different known vulnerabilities. Specifically the exploits leveraged CVE-2012-0158, CVE-2013-3906 and CVE-2014-1761. Secondarily the attackers also leveraged drive-by web attacks through the usage of known exploit toolkits, RedKit and Null. After the initial exploitation of a victim the attackers would then look to install the malware now known as Carbanak. In some of the early breaches the Carbanak gang leveraged malware based on Carberp but as they progressed overtime the malware used by Carbanak became wholly its own and was no longer based on Carberp. For completeness you will find at the end of this document a reference to some of the vulnerabilities also leveraged by Carberp. In the case of the Carbanak malware in some scenarios the malware would try to leverage second-stage exploits in order to gain increased privileges on a machine. Specifically the attackers were known to exploit a Microsoft local privilege escalation exploit, CVE-2013-3360. This would allow the attackers in some instances to go from a standard user account to that of a local system/administrator equivalent account which would have full control over a victim machine. Kaspersky notes the malware itself would copy itself to %system32%com with a file name of svchost.exe. This is to be understood that the malware would copy itself to the Windows system32 folder. The malware would also create a new Windows service on the system and enable Remote Desktop (RDP) to be automatically started. These characteristics of course require Administrator or equivalent level of privilege on a system. So in cases where the attackers did not leverage a secondary privilege escalation exploit or that such an exploit would have failed – a least privilege environment would have helped mitigate this malware from being able to execute properly. While information is not specific in all cases as to how lateral movement was made from initially compromised machines to financial systems, such as money processing and related systems, it serves as a prudent reminder of how common it is for attackers to gain a foothold, steal existing user accounts and privileges, and then leverage those accounts as a user would but to a malicious end. Proper logging and auditing of accounts, privileged accounts and passwords can help to create an early warning mechanism for such activity. Lastly given the attackers were leveraging known vulnerabilities it serves as a critical reminder of the importance of a proper vulnerability and patch management process to prioritize vulnerabilities for remediation which can therefore properly close the initial point of entry used in a variety of attacks. We have included for reference a list of Retina vulnerability audits which customers can use to verify that they are properly patched against exploits used within Carbanak. Also given the attackers leveraged email phishing attacks with .CPL (Control Panel) file attachments organizations should verify that they are filtering such file types both within network perimeter, web and email filtering solutions. This has been a recommended file type to block for many years now. In the end it is clear that these attackers were fluid in the tools and techniques that they leveraged but overall the attacks represent a formula that continues to be common in how breaches occur. While proper management of vulnerabilities and privileges alone will not 100% secure an environment it is increasingly apparent that threat prevention and detection strategies must include aspects of privileges and vulnerabilities as they are two components leveraged in almost every breach. Retina Vulnerability Audit References: Carbanak Point of Entry CVE-2012-0158 16213 - Microsoft Windows Common Controls Code Execution (2664258) 16214 - Microsoft Windows Common Controls Code Execution (2664258) - x64 CVE-2013-3906 31830 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Office 2003 31831 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Office 2007 31832 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Office 2010 31833 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync 2013 31835 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Vista/2008 31836 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync 2010 31837 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync Attendee (User) 31838 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync Attendee (Admin) 31844 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync 2010 x64 31845 - Microsoft Windows GDI+ Remote Code Execution (2908005) - Lync 2013 x64 CVE-2014-1761 33598 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2863907 33599 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2863910 33600 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878303 33605 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878237 33610 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878304 33611 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878236 33612 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878221 33613 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878220 33614 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2878219 33615 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2863919 33616 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) KB2863926 33619 - Microsoft Word and Office Web Apps Multiple Vulnerabilities (2949660) 2878236-W8 Carbanak Privilege Escalation CVE-2013-3660 19520 - Microsoft Windows Kernel-Mode Drivers Remote Code Execution (2850851) Carbanak RDP enabled 1408 - Terminal Services enabled Carberp Privilege Escalation CVE-2012-0217 16553 - Microsoft Windows Kernel Privilege Escalation (2711167) CVE-2012-1864 16551 - Microsoft Windows Kernel Mode Drivers Multiple Vulnerabilities (2709162)

Scott Lang

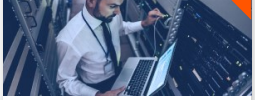
Sr. Director, Product Marketing at BeyondTrust

Scott Lang has nearly 20 years of experience in technology product marketing, currently guiding the product marketing strategy for BeyondTrust's privileged account management solutions and vulnerability management solutions. Prior to joining BeyondTrust, Scott was director of security solution marketing at Dell, formerly Quest Software, where he was responsible for global security campaigns, product marketing for identity and access management and Windows server management.

You May Also Be Interested In:

Webcasts | April 14, 2020

How to Vanquish Critical IT Vulnerabilities!



Webcasts | April 01, 2020

LATAM | Por qué Administrar las Contraseñas ya no es Suficiente: un Enfoque Universal para PAM

Whitepapers

Privileged Password Management Explained

BeyondTrust

Keep up with BeyondTrust

Work Email

Subscribe

I agree to receive product related communications from BeyondTrust as detailed in the Privacy Policy, and I may manage my preferences or withdraw my consent at any time.

Customer Support

Contact Sales

Products

- Endpoint Privilege Management
- Password Management
- Privileged Remote Access
- DevOps Secrets Safe
- Remote Support

Resources

- Blog
- Case Studies
- Competitor Comparisons
- Datasheets
- Glossary
- Videos
- Webcasts
- Whitepapers

About

- Company
- Careers
- Contact
- Events
- Leadership Team
- Partner Program
- Press

Languages

- English
- German
- French
- Spanish
- Korean
- Portuguese
- Japanese

Privacy | Security | Manage Cookies | WEEE Compliance