Cyber Threats and Mitigation Measures for High Net-Worth Individuals

Information as of 18 September 2015—1700 hours EST

Disclaimer: *This report represents work derived from various sources. The information contained herein is the best available to Red Five Security, LLC (Red Five) in the open source arena on short notice. However, it may be based in part on information provided by third party sources. Therefore, Red Five accepts no liability for the accuracy or integrity of the information. The condition of the information mentioned in this report may change at any time. The report is intended for the exclusive use of the addressee and is intended for informational purposes only. This report may not be used in a legal proceeding without the permission of Red Five.*

Cyber threats are quickly becoming one of the most prevalent security threats to high net-worth individuals, especially as more information is posted and stored online. Criminals compromised the personal records of more than 117 million people in the first six months of 2015, according to the Identity Theft Resource Center.

- Cybercrime costs the global economy $300 billion annually, with $100 billion concentrated in the United States, according to a 2015 Center for Strategic and International Studies report.
- Mobile device vulnerabilities, scams, targeted attacks, and data breaches all pose a substantial threat to high net-worth individuals.

Mobile Devices and the "Internet of Things"

Threat

As technology drives more web activity to smartphones, cybercriminals have increased their focus on compromising these devices, which may contain sensitive and personal data. The number of mobile device attacks increased rapidly from 2013 to 2014, up approximately tenfold to 644,000 attacks per month by March 2014, according to an October 2014 Kaspersky Lab study.

- Kaspersky Lab estimates that 98 percent of all existing mobile malware targets the users of Android devices, which make up approximately 85 percent of the mobile market.
- Symantec's Norton Mobile Insight determined nearly one million Android applications—approximately one in seven—are malware. Symantec determined another 2.3 million Android applications are "grayware," which do not contain viruses but can be annoying to the user.
- The Kaspersky Lab study also reports that 59 percent of detected malware relates directly to programs capable of stealing users money. Approximately 35 percent of US adults bank on mobile devices.

Attackers can also target and hack into smart devices or use them as a point of access to a personal network; these devices are rarely part of any security system. The "Internet of Things" refers to the connectivity of various devices to the larger network that has traditionally been the exclusive domain of computers. Now—especially in the homes of high net-worth individuals—lighting, heating, and cooling systems; car navigation and entertainment systems; appliances; TVs; and a number of other devices may be connected to the Internet for different purposes.

- A 2014 Hewlett-Packard security study revealed that 70 percent of "Internet of Things" devices were vulnerable to attack, with an average of 25 vulnerabilities per product.
- Computer scientists in 2015 revealed that they could remotely hijack a Jeep through Fiat Chrysler's Uconnect system and kill the engine, disable the breaks, and even take control of the steering. The carmaker recalled 1.4 million vehicles after the demonstration.

Mitigation

Download trusted applications and limit the sensitive activities that take place on your mobile devices. While malware exists for all mobile operating systems, Android is by far the most vulnerable due to its susceptibility of system attacks and viruses. Because Apple fully vets all applications before they are available on the App Store, iOS products—such as the iPhone and the iPad—are generally more secure than their Android counterparts.

- Updating mobile device software as soon as new updates are issued will prevent some security issues. A large percentage of network security issues can be avoided through the timely application of patches, which correct known software vulnerabilities.
- Limit the devices that connect to your residential network to those that are known to limit points of vulnerability. IT professionals should actively scan the network on a monthly basis to search for new and unregistered devices.
- Consider the installation of an Intrusion Detection and Notification system for the IT Ethernet network and an applications-based firewall to protect the network.

Scams

Threat

Online criminals have begun to favor social media over traditional email for scam efforts, as these platforms have grown in popularity in recent years. Scammers take advantage of "social proof," which means that people believe in

the validity of something if it is shared by others. They hijack real user accounts on social media networks and endorse a scam product or link.

- Approximately 70 percent of social media scams take advantage of this idea and rely on "manual sharing," where unwitting victims spread fake offers amongst their friends, according to the 2015 Symantec Internet Security Threat Report.
- Scammers took advantage of the death of Robin Williams by sharing his alleged "goodbye video," which people shared on social media. There was no video, but rather the link brought users to sites to fill out surveys or download software.
- One in 965 emails in 2014 were phishing scams, according to Symantec. This number is down from one in 392 in 2013.

Mitigation

Exercise caution when following links on social media sites or in emails, as they could be scams.

- Enable your email server so that it disables auto-clicking on links will protect against some phishing scams and other unsolicited emails.

Targeted Attacks

Threat

Targeted attacks tend to focus on industry and government, but may also include individuals, especially those who have a high profile or substantial wealth. Targeted attacks are more pointed and direct than the broad-spectrum malware that traditionally infects web devices. While these attacks are normally used for corporate or diplomatic espionage, high net-worth individuals may become the target if the goal is extortion or gaining access to an individual's private data. Hacktivists, criminal extortionists, and data thieves may all carry out targeted attacks.

- Hackers extort more than $5 million from victims each year, according to a 2014 Symantec Report.
- Cybercriminals released almost 200 private celebrity photographs online in August 2014 using targeted attacks on their individual accounts.

Ransomware

Targeted attacks may feature "ransomware" that remotely locks an individual's device or restricts access to user files until a payment is made. Ransomware attacks increased more than 100 percent from 4.1 million attacks in 2013 to 8.8 million in 2014—about 24,000 per day—according to Symantec. The

attackers usually demand between $300 and $500 in Bitcoin or untraceable MoneyGram for the return of the victim's device or files, but once it is clear that the victim will pay, the attacker may continue to demand funds, with ransoms sometimes exceeding $10,000. CryptoWall Ransomware, a specific type of the attack, resulted in $18 million in losses for victims between April 2014 and June 2015, according to the FBI Internet Crime Complaint Center.

Performing nightly backups of workstations and servers, and maintaining up-to-date anti-malware software can mitigate some threat of ransomware. Backing up workstations provides access to files even if the primary source is taken hostage by hackers.

Mitigations

Spear-phishing is the most common type of targeted attack and can be mitigated by awareness of unusual emails. Spear-phishing emails often appear to be from a colleague or corporation known by the target, but contain an attachment that is actually a virus or Trojan. These programs can then provide access to data on the users system for the hacker.

- Be aware of emails that you are not expecting that contain attachments; verify the validity of the attachment from the sender prior to opening it. If the message appears suspicious, do not open the attachment.
- Files with the extensions ".doc" and ".exe" are the most common types used in spear-phishing efforts, making up 61 percent of all email attachments used in targeted attacks, according to the 2015 Symantec Internet Security Threat Report.

Data Breaches

Threat

Data breaches are becoming increasingly common and cyber criminals can use compromised information for identity theft. Hackers breached 312 databases in 2014, up 23 percent from 2013, according to the Symantec Internet Security Threat Report. Healthcare was the most common sector targeted for cybercrime, followed by retail, education, government, and finance. The information most frequently exposed was names; government ID numbers, such as social security numbers; home addresses; financial information; and birth dates—all of which can be used for identity theft.

- Cybercriminals exposed an average of 1.1 million identities in each breach in 2015, according to the Symantec Internet Security Threat Report. The average cost of a corporate data breach in 2014 was $3.79 million, according to a 2015 IBM and Ponemon Institute study.

- Hackers stole the sensitive information of 21.5 million US government employees and applicants from the Office of Personnel Management database. The breach began in 2014, but the government did not detect it until April 2015.
- Attacks on Home Depot and Target in 2014 exposed ten of millions of customers' personal information, including credit card data.

Mitigation

Limit the personal information given to online services and frequently monitor your credit score and bank accounts for signs of identity theft. Only submit the minimum necessary personal information to databases and online accounts.

- Some, although not all, organizations and corporations will publicize when hackers breach their database. It is important to monitor these announcements and determine if and how your private information may have been compromised.
- Unauthorized withdrawals from bank accounts, debt collectors calling about debts that aren't yours, unfamiliar accounts or charges on your credit report, and the IRS notifying about more than one tax return filed in your name may all be signs that your identity has been stolen.