

Security Now! #439 - 01-21-14

Q&A #181

Link Tracking Warning!

This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This Week on Security Now!

- Barack's Friday "Do Nothing" NSA speech,
- The Windows XP Target POS malware,
- Revisiting CryptoLocker (some execution details & how much did the bad guys make?),
- My TSA interview... and a better alternative,
- A terrific free eMail archiving solution,
- GRC's quantum-tunneling true hardware random number generator,
- An update on SQRL's password encryption technology,
- ... and a Q&A with our listeners!

Security News:

Obama's Friday NSA Reform speech

- <http://bit.ly/bo-nsa>
- <https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained>

TARGET breach Malware

- <http://www.nydailynews.com/news/world/russian-teen-made-target-neiman-marcus-malware-report-article-1.1583785>

Sergey Taraspov



- A different 23-year old confessed to be the original developer
- "BlackPOS" a windows trojan a memory scrapper
- ANY version of Windows / The POS terminals run a customized version of XP Embedded.
- "OpenProcess" and obtain a handle that provides access to the process memory.
- The malware was apparently carefully design specifically for the Target breach.
- Even as late as Jan 16th, *zero* anti-malware software recognizes it.
- Seculert's Research Lab ran the sample of the malware and discovered that this attack had 2 stages, which is a well known attribute of an advanced threat. First, the malware that infected Target's checkout counters (PoS) extracted credit numbers and sensitive personal details.

Then, after staying undetected for 6 days, the malware started transmitting the stolen data to an external FTP server, using another infected machine within the Target network.

That FTP server appears to be on a hijacked website. These transmissions occurred several times a day over a 2 week period.

At this time, the cyber criminals behind the attack used a virtual private server (VPS) located in Russia to download the stolen data from the hijacked FTP server. They continued to download the data over 2 weeks for a total of 11 GBS of stolen sensitive customer information. While none of this data remains on the FTP server today, analysis of publicly available access logs indicates that Target was the only retailer affected. So far there is no indication of any relationship to the Neiman Marcus attack.

- Rumors of SIX other retailers, beyond Target and Neiman Marcus, are emerging.

CryptoLocker Update:

Keith Jarvis, Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence

<http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/>

Crypto:

Instead of using a custom cryptographic implementation like many other malware families, CryptoLocker uses strong third-party certified cryptography offered by Microsoft's CryptoAPI. By using a sound implementation and following best practices, the malware authors have created a robust program that is difficult to circumvent. The malware uses the "Microsoft Enhanced RSA and AES Cryptographic Provider" (MS_ENH_RSA_AES_PROV) to create keys and to encrypt data with the RSA (CALG_RSA_KEYX) and AES (CALG_AES_256) algorithms.

The encryption process begins after CryptoLocker has established its presence on the system and successfully located, connected to, and communicated with an attacker-controlled C2 server. This communication provides the malware with the threat actors' RSA public key, which is used throughout the encryption process.

Drives:

The malware begins the encryption process by using the GetLogicalDrives() API call to enumerate the disks on the system that have been assigned a drive letter (e.g., C:). In early CryptoLocker samples, the GetDriveType() API call then determines if the drives are local fixed disks or network drives (DRIVE_FIXED and DRIVE_REMOTE, respectively). Only those two types of drives are selected for file encryption in early samples. Samples since late September also

select removable drives (DRIVE_REMOVABLE), which can include USB thumb drives and external hard disks.

After selecting a list of disks to attack, the malware lists all files on those disks that match the 72 file patterns shown in Table 2. Over time, the threat actors adjusted which types of files are selected for encryption; for example, PDF files were not encrypted in very early samples but were added in mid-September. As a result, the list in Table 2 is subject to change.

Action:

Each file is encrypted with a unique AES key, which in turn is encrypted with the RSA public key received from the C2 server. The encrypted key, a small amount of metadata, and the encrypted file contents are then written back to disk, replacing the original file. Encrypted files can only be recovered by obtaining the RSA private key held exclusively by the threat actors.

As a form of bookkeeping, the malware stores the location of every encrypted file in the Files subkey of the HKCU\SOFTWARE\CryptoLocker (or CryptoLocker_0388) registry key

After finishing the file encryption process, CryptoLocker periodically rescans the system for new drives and files to encrypt.

The malware does not reveal its presence to the victim until all targeted files have been encrypted. The victim is presented with a splash screen containing instructions and an ominous countdown timer

Payment:

The ransom amount varied in very early samples (see Table 3), but settled at \$300 USD or 2 BTC (Bitcoins) within the few weeks after CryptoLocker's introduction. Dramatic Bitcoin price inflation in the latter months of 2013 prompted the threat actors to reduce the ransom to 1 BTC, 0.5 BTC, and then again to 0.3 BTC, where it remains as of this publication.

Current payment options:

Although early versions of CryptoLocker included numerous payment options, the threat actors now only accept MoneyPak and Bitcoin. The Bitcoin option was originally marketed as the "most cheap option" [sic] for ransom payment based on the difference between the \$300 USD ransom and the market rate of Bitcoins. From August to December 2013, the Bitcoin market experienced major volatility and dramatically increased in price, negating any monetary benefits for victims to choose this payment method.

The variety of payment options and currency choices in early CryptoLocker versions suggests the threat actors originally anticipated a global infection pattern. For reasons unknown to CTU researchers, the threat actors elected to focus exclusively on English-speaking countries and removed the payment options less popular in these countries.

Anecdotal reports from victims who elected to pay the ransom indicate that the CryptoLocker threat actors honor payments by instructing infected computers to decrypt files and uninstall the malware. Victims who submit payments are presented with the payment activation screen shown in Figure 9 until the threat actors validate the payment. During this payment validation phase, the malware connects to the C2 server every fifteen minutes to determine if the

payment has been accepted. According to reports from victims, payments may be accepted within minutes or may take several weeks to process.

How Much Money Was Extorted?

<http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/>

- 200,000 and 250,000 infections
-
- In research for this article ZDnet traced four bitcoin addresses posted (and re-posted) in forums by multiple CryptoLocker victims, showing movement of 41,928 BTC between October 15 and December 18.
-
- Based upon the current BTC of \$960, this is \$40,250,880 USD.

Carbonite:

Carbonite was reported in November to have been dealing with "several thousands" of phone calls from CryptoLocker-infected victims, and now have a dedicated team dealing with CryptoLocker recoveries.

Miscellany:

TSA Update from Evan Katz:

- Links for Leo:
- <http://www.globalentry.gov/howtoapply.html>
- <http://www.globalentry.gov/enrollmentcenters.html>

Subject: Your Comments re Pre Check

Hi Leo.

Re: TSA pre-check, you probably do *not* want to get it. Rather, you and your family and friends should do the global entry program run by the Department of Homeland Security.

The reason why you want to do global entry and not pre-check is a global entry includes very expedited coming back into the US from overseas and pre-check does not. Moreover the DHS program has many more locations that you can go to, which will be much closer to where you live.

And the DHS program costs only \$15 more then recheck. That is, the global entry program costs \$100 for five years where as the pre-check program cost \$85 for five years. And global entry is accepted at all pre-check locations.

I hope that all is well with you, and wish you all the best in the new year and 2014!
Best regards, Evan

"MailStore Home"

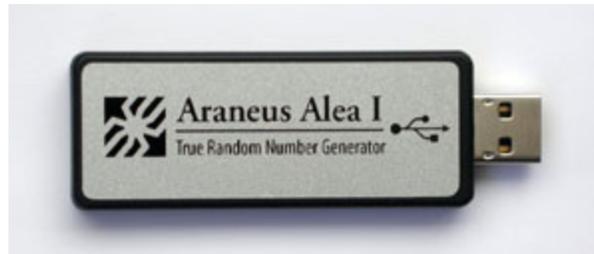
- <http://www.mailstore.com/>
- 219,105 messages / 945MB
- When you want to keep everything "offline" but instantly indexed and findable.
- Archive from:
 - Online Accounts: Microsoft Exchange, Google Mail, IMAP, POP3 and others.
 - Outlook, Outlook Express, Windows Live Mail, Thunderbird, SaeMonkey
 - EML & MSG files and MBOX files.
- Export to:
 - Online: Exchange Mailbox, IMAP, eMail address via SMTP
 - Outlook, Outlook Express, Thunderbird, SeaMonkey
 - File system Email files.

Jack Ryan: Shadow Recruit (Chris Pine)

- Patriot Games (Harrison Ford)
- The Hunt for Red October (Alec Baldwin)
- Clear and Present Danger (Harrison Ford)
- The Sum of All Fears (Ben Affleck)

GRC to get TRUE "Quantum" Random numbers...

<http://www.araneus.fi/products-alea-eng.html>



<quote> The Alea I uses a reverse biased semiconductor junction to generate wide-band Gaussian white noise. This noise is amplified and digitized using an analog-to-digital converter. The raw output bits from the A/D converter are then further processed by an embedded microprocessor to combine the entropy from multiple samples into each final output bit, resulting in a random bit stream that is practically free from bias and correlation.</quote>

SpinRite:

Anonymity requested for podcast:

Thanks again for a great tool. I use it on all of my drives personal. It has even brought back some drives that were getting recycled. If I came across a disk that failed a DBAN DoD wipe, I would run the disk on SpinRite at level one until completed. Then if it failed DBAN again I would run the disk through SpinRite at level 2. If again the disk failed at DBAN, it would be run at SR level 4. Only 1 drive out of 100 (literally) needed a drilled-platter treatment. For every other dead drive, SpinRite was able to bring it back to life for DBAN wiping.

PS. please keep my name off air for this testimonial. Thank you.

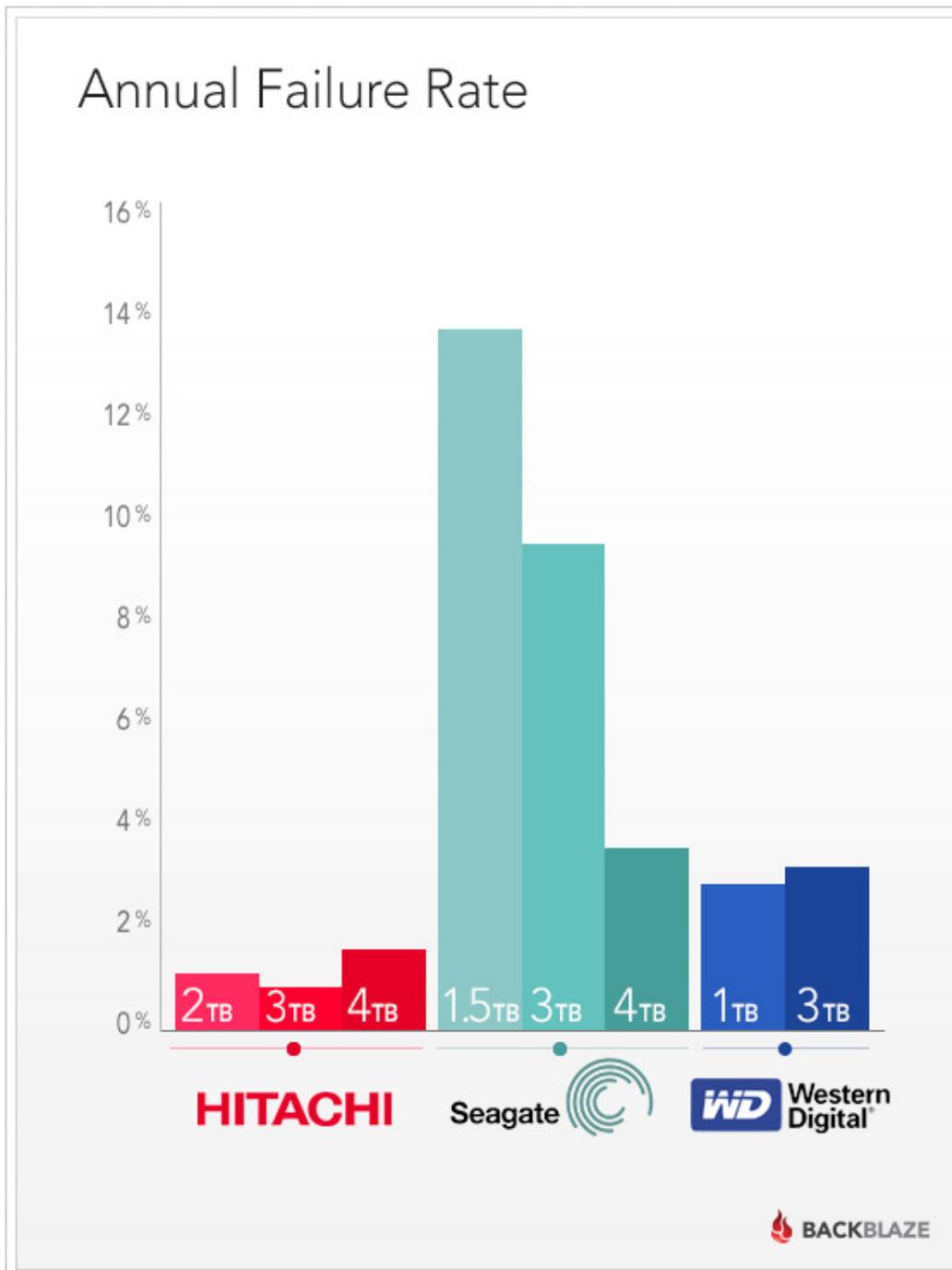
Notes: DBAN - Darik's Boot and Nuke.

"Beyond Recall" will follow SR v6.1 ("the gang" strongly didn't want it built into SR.)

Hard Drive Reliability Update:

<http://www.zdnet.com/who-makes-the-best-disk-drives-7000025375/>

<http://blog.backblaze.com/2014/01/21/what-hard-drive-should-i-buy/>



SQLR Status:

- Scrypt and Memory-Hardness
- Resisting hardware acceleration attacks
- Scrypt N, r, p parameters
- SQLR: Chaining Scrypt and XORing all outputs

Errata:

- The "C" in the acronym "COTS" stands for "Commercial", not "Common".