TREND MICRO | TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

New Version of Cerber Ransomware Distributed via Malvertising

- Posted on:August 31, 2016 at 8:28 pm
- Posted in:Exploits, Malware, Ransomware
- Author:
  Joseph C Chen (Fraud Researcher)

0

Cerber has become one of the most notorious and popular ransomware families in 2016. It has used a wide variety of tactics including leveraging cloud platforms and Windows Scripting and adding non-ransomware behavior such as distributed denial-of-service attacks to its arsenal. One reason for this popularity may be because it is frequently bought and sold as a service (ransomware-as-a-service, or RaaS).

The latest version of Cerber had functions found in earlier versions like the use of voice mechanism as part of its social engineering tactics. Similar to previous variants, Cerber 3.0 is dropped by the Magnitude and Rig exploit kits.

Users are typically redirected to these exploit kit servers via ads appearing in a pop-up window after clicking a video to play. This ultimately leads to the download of Cerber. While this malvertisment campaign has affected several countries already, the attack is heavily concentrated in Taiwan. And although this malvertising campaign has been running for months, it was only now that it dropped Cerber 3.0 as its payload.

In the case of Magnitude, a simple redirect script was used. Rig, on the other hand, opened a website in the background that contained a screenshot of legitimate US clothing shopping sites, perhaps to make the ad look less suspicious.

#	Result	Protocol	Host	URL	Comments	Content-Type
50	200	HTTP	[redacted]	/adsprp.php		text/html; charset=UTF-8
51	301	HTTP		[redacted]		text/html; charset=UTF-8
52	200	HTTP	onclickads.net	/afu.php?zoneid=297420	Advertising Network	text/html
53	302	HTTP	onclickads.net	/?r=%2Fmb%2Fhan&zonei...	Advertising Network	text/html
54	303	HTTP	bid.ams01.wwwpromoter.com	/attribution/12463/34729?d...	Advertising Network	text/plain; charset=utf-8
55	303	HTTP	creative.ams01.wwwpromoter.com	/pop-imp/12463/34729?devi...	Advertising Network	text/plain; charset=utf-8
56	302	HTTP	yesstyle.onlineshoptadviser.info	/g/rug83ugoiaosigk18sf83tj...	Malvertising	text/html; charset=UTF-8
57	302	HTTP	yesstyle.onlineshoptadviser.info	/promoter15.html	Malvertising	text/html; charset=iso-8859-1
58	200	HTTP	yesstyle.onlineshoptadviser.info	/g/rug83ugoiaosigk18sf83tj...	Malvertising	text/html
59	200	HTTP	armenlab.pw	/rpgojekfn10.html	Malvertising	text/javascript
60	200	HTTP	yesstyle.onlineshoptadviser.info	/g/rug83ugoiaosigk18sf83tj...	Malvertising	image/png
61	200	HTTP	we.approved203kcontractors.com	/?wX6OcbiYLB_LCYY=l3SKfP...	Rig Exploit Kit	text/html

Figure 1. Rig exploit kit redirection chain

#	Result	Protocol	Host	URL	Comments	Content-Type
1	200	HTTP	[redacted]	/adsprp.php		text/html; charset=UTF-8
2	301	HTTP		[redacted]		text/html; charset=UTF-8
3	200	HTTP	onclickads.net	/afu.php?zoneid=297420	Advertising Network	text/html
4	302	HTTP	onclickads.net	/?r=%2Fmb%2Fhan&zoneid...	Advertising Network	text/html
5	302	HTTP	xml.pdn-2.com	/click?adv=30402&i=KPF3PJJ...	Advertising Network	
6	200	HTTP	plannetgamework.org	/	Malvertising	text/html
7	200	HTTP	7bb1ybl2cbi20pd2ax.didartist.vip	/?availHeight=728&availWidt...	Malvertising	text/html
8	200	HTTP	ffu7p5s215t3bebf9.drewcares.bid	/?2d5f484b42434e41444e46...	Magnitude Exploit Kit	text/html

Figure 2. Magnitude exploit kit redirection chain

Beyond those differences, however, Cerber remains the same. The initial ransom note uses wording that is essentially unchanged from previous versions:

CERBER RANSOMWARE

Cannot you find the files you need?
Is the content of the files that you looked for not readable?

It is normal because the files' names, as well as the data in your files have been encrypted.

Great!
You have turned to be a part of a big community "#C3rber Ransomware".

Figure 3. Cerber 3.0 ransom note

The payment note is also similar to earlier variants, even offering a "discount". Perhaps to reflect the ever-changing exchange rate of Bitcoins, the amount demanded has also changed. In the first version, Cerber demands 1.24 BTC (~US$523, as of March 4, 2016) and gave affected entities seven days. Cerber 3.0 asks for 1 BTC right away, but if the user waits more than five days the ransom doubles to 2 BTC.

Figure 4. Cerber version 3 ransom note

The encrypted files are renamed to have the **.cerber3* file extension. Shadow copies are also deleted by the ransomware, to prevent any backups based on this feature from being restored. It also uses a female voice to let users know that their files have been encrypted—like the initial version of Cerber did.

Solutions and Mitigation

The most fundamental defense against ransomware is still backing up. With proper backups in place, organizations need not worry about any data loss that may be incurred. At the very least, important files should be backed up on a regular basis. Practice the 3-2-1 rule wherein 3 copies are stored in two different devices, and another one to a safe location.

A good defense against malvertising (and exploit kits in general) is to keep the software in use up-to-date with all security patches. This will reduce the risk against a wide variety of attacks, not just ransomware. This includes both the operating system and any applications in use. A security solution that can proactively provide defense against attacks targeting vulnerabilities in the system's software is also recommended.

Trend Micro offers solutions that protect users and organizations in all aspects –at the gateway, endpoints, networks, and even servers.

PROTECTION FOR ENTERPRISES

- **Email and Gateway Protection**

Trend Micro Cloud App Security, Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security address ransomware in common delivery methods such as email and web.

Spear phishing protection
Malware Sandbox
IP/Web Reputation
Document exploit detection

- **Endpoint Protection**

Trend Micro Smart Protection Suites detects and stops suspicious behavior and exploits associated with ransomware at the endpoint level.

Ransomware Behavior Monitoring
Application Control
Vulnerability Shielding
Web Security

- **Network Protection**

Trend Micro Deep Discovery Inspector detects malicious traffic, communications, and other activities associated with attempts to inject ransomware into the network.

Network Traffic Scanning
Malware Sandbox
Lateral Movement Prevention

- **Server Protection**

Trend Micro Deep Security™ detects and stops suspicious network activity and shields servers and applications from exploits.

Webserver Protection
Vulnerability Shielding
Lateral Movement Prevention

PROTECTION FOR SMALL-MEDIUM BUSINESSES AND HOME USERS

- **Protection for Small-Medium Businesses**

Trend Micro Worry-Free™ Business Security Advanced offers cloud-based email gateway security through Hosted Email Security that can detect and block ransomware.

Ransomware behavior monitoring
IP/Web Reputation

- **Protection for Home Users**

Trend Micro Security 10 provides robust protection against ransomware by blocking malicious websites, emails, and files associated with this threat.

IP/Web Reputation
Ransomware Protection

The following SHA1 hashes were involved in this attack:

- C60AB834453E6C1865EA2A06E4C19EA83982C1F9 – detected as RANSOM_CERBER.DLEY
- E9508FA87D78BC01A92E4FDBCD3D14B2836BC0E2 – detected as RANSOM_CERBER.DLEZ

Additional analysis by Mary Yambao

Updated on September 1, 2016, 7:00 PM (UTC-7):

Figure 1 and Figure 2 were updated.

Updated on September 6, 2016, 2:15 AM (UTC-7):

Ransom_CERBER.DLEY has been renamed to Ransom_CERBER.DLEZ.

Related Posts:

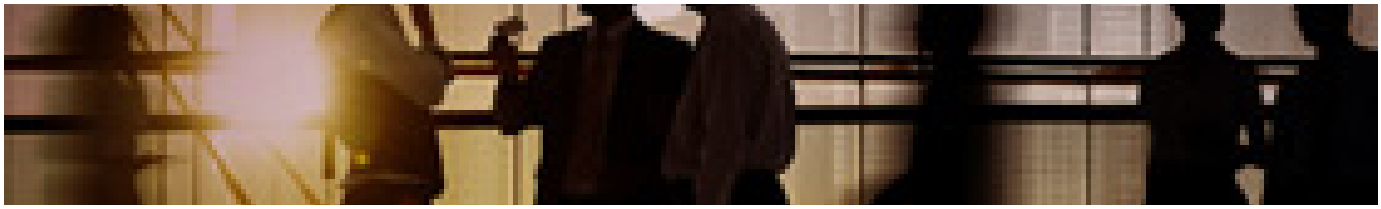
- **CERBER: Crypto-ransomware that Speaks, Sold in Russian Underground**
- **Cerber: A Case in Point of Ransomware Leveraging Cloud Platforms**
- **After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity**
- **Chinese-language Ransomware 'SHUJIN' Makes An Appearance**

Tags: CERBERMagnitude exploit kitmalvertisingransomwarerig exploit kit

Featured Stories

- Microsoft Patches IE/Edge Zero-day Used in AdGholas Malvertising Campaign
- CVE-2016-6662 Advisory: Recent MySQL Code Execution/Privilege Escalation Zero-Day Vulnerability
- BkSoD by Ransomware: HDDCryptor Uses Commercial Tools to Encrypt Network Shares and Lock HDDs
- The French Dark Net Is Looking for Grammar Police
- Pokémon-themed Umbreon Linux Rootkit Hits x86, ARM Systems

Business Email Compromise



- How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
  See the numbers behind BEC

Latest Ransomware Posts

How Stampado Ransomware Analysis Led To Yara Improvements

The Rise and Fall of Encryptor RaaS

From RAR to JavaScript: Ransomware Figures in the Fluctuations of Email Attachments

A Show of (Brute) Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses

BkSoD by Ransomware: HDDCryptor Uses Commercial Tools to Encrypt Network Shares and Lock HDDs

Recent Posts

- FastPOS Updates in Time for the Retail Sale Season
- How Stampado Ransomware Analysis Led To Yara Improvements
- Helper for Haima iOS App Store Adds More Malicious Behavior
- DressCode and its Potential Impact for Enterprises
- The Rise and Fall of Encryptor RaaS

Ransomware 101

- 

  This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
  Check the infographic

Popular Posts

Pokémon-themed Umbreon Linux Rootkit Hits x86, ARM Systems
DressCode and its Potential Impact for Enterprises
BkSoD by Ransomware: HDDCryptor Uses Commercial Tools to Encrypt Network Shares and Lock HDDs
CVE-2016-6662 Advisory: Recent MySQL Code Execution/Privilege Escalation Zero-Day Vulnerability
New Version of Cerber Ransomware Distributed via Malvertising

Latest Tweets

- Affiliates of #Encryptor #RaaS get to keep 95% of the profit per victim. More on its modus operandi: bit.ly/2dtBNOJ
  about 3 hours ago
- #Crysis veers away from usual infection vectors and instead uses RDP brute force. Our recent #ransomware detections: bit.ly/2cXU2uJ
  about 7 hours ago
- Stolen #PII can range from corporate credit card details to online credentials. How cybercriminals earn from them:… twitter.com/i/web/status/7…
  about 11 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe