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

Several Exploit Kits Now Deliver Cerber 4.0

- Posted on:October 12, 2016 at 5:05 am
- Posted in:Bad Sites, Ransomware, Vulnerabilities
- Author:
  Joseph C Chen (Fraud Researcher)

0

We have tracked three malvertising campaigns and one compromised site campaign using Cerber ransomware after version 4.0 (detected as as Ransom_CERBER.DLGE) was released a month after version 3.0. More details of this latest iteration of Cerber are listed in a ransomware advertisement provided by security researcher Kafeine.

The upgrades include shifting their ransom note to *.hta* format from html. The ransomware authors have also stopped using the consistent string ".cerber3" as the extension for encrypted files, and have turned to using random string generated for each infection as the new file extension. Based on the speedy adoption of Cerber 4.0—which has been seen in the wild since the start of October—the upgrades seem to have caught the attention of cybercriminals.

The advertisement reads:

Cerber Ransomware 4.0	***Cerber Ransomware 4.0 (translated)***
– FUD на топовых антивирусах (скантайм / рантайм)	– FUD at the top antivirus (skantaym / runtime)
– Обход мониторинга активности (массовое изменение, обход ханипотов итд.)	– Bypass activity monitoring (weight change, bypassing the Honeypot, etc.)
– Обход всех известных anti-ransomware программ	– Bypass all known anti-ransomware programs
– Работает 5 крипторов 7 дней в неделю	– Works 5 cryptors 7 days a week
– Обновленный морф	– Updated morph
– Новые инструкции на 13 языках + новый фон	– New instructions in 13 languages + new background
– Синхронизация доменов через блокчейн (больше не важно забанили домен лендинга или нет)	– Synchronization via the domain blokcheyn (no longer important domain Landing banned or not)
– Рандомное расширение для шифрованных файлов, обновленный алгоритм шифрования	– Randomly extension for encrypted files, the updated encryption algorithm
– Новые типы файлов для шифрования	– New types of files to encrypt
– Закрытие запущенных процессов всех топовых баз данных	– Closing all running processes top database
– Обновленный JS Loader	– Updated JS Loader
– Новые onion домены и многое другое.	– New onion domains and much more.

The quick popularity of Cerber 4.0

As we reported previously, Cerber has become one of the most prominent ransomware families of 2016. It has a wide range of capabilities and is often bought and sold as a service (ransomware-as-a-service or RaaS)—even earlier versions were peddled as RaaS in underground markets. The rapid release of Cerber updates have made it an increasingly popular payload for several exploit kits. This follows our research, which shows exploit kits continuously adopt ransomware families to target new vulnerabilities.

One campaign that seems to favor the latest version of Cerber is PseudoDarkleech, a continuously changing campaign that mostly delivers ransomware through compromised sites. It previously distributed CrypMIC and CryptXXX, but Trend Micro researchers noted that PseudoDarkleech switched to Cerber 4.0 last October 1.

#	Result	Protocol	Host	URL	Comments	Body	Content-Type
1	200	HTTP	[redacted]	/	Compromised Site (PseudoDarkleech)	5,998	text/html; charset=utf-8
2	200	HTTP	add.usaviatorfinancing.net	/?xHiNdbSdLR7KC4c=l3SKfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu...	Rig Exploit Kit	18,650	text/html; charset=UTF-8
3	200	HTTP	add.usaviatorfinancing.net	/index.php?xHiNdbSdLR7KC4c=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKrXCJ-ofSih17O...	Rig Exploit Kit	21,706	application/x-shockwave-flash
5	200	HTTP	add.usaviatorfinancing.net	/index.php?xHiNdbSdLR7KC4c=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKrXCJ-ofSih17O...	Rig Exploit Kit	21,706	application/x-shockwave-flash
8	200	HTTP	add.usaviatorfinancing.net	/index.php?xHiNdbSdLR7KC4c=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKrXCJ-ofSih17O...	Rig Exploit Kit (Drop: Cerber)	312,487	application/x-msdownload

Figure 1. This version of PseudoDarkleech directly injects the RIG exploit kit link onto the compromised site

#	Result	Protocol	Host	URL	Comments	Body	Content-Type
1	200	HTTP	[redacted]	/contact/	Compromised Site	39,964	text/html; charset=UTF-8
64	200	HTTP	praijn.ddnsking.com	/wordpress/?ARX8	Dynamic DNS redirect gate	331	text/html
80	200	HTTP	re.flighteducationfinancecompany.com	/?wXaJcLWZKxjJCYU=l3SKfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKrXCJ-ofSih1...	Rig Exploit Kit	18,521	text/html; charset=UTF-8
85	200	HTTP	re.flighteducationfinancecompany.com	/index.php?wXaJcLWZKxjJCYU=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKr...	Rig Exploit Kit	21,706	application/x-shockwave-flash
92	200	HTTP	re.flighteducationfinancecompany.com	/index.php?wXaJcLWZKxjJCYU=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKr...	Rig Exploit Kit	21,706	application/x-shockwave-flash
100	200	HTTP	re.flighteducationfinancecompany.com	/index.php?wXaJcLWZKxjJCYU=l3SMfPrfJxzFGMSUb-nJDa9BNUXCRQLPh4SGhKr...	Rig Exploit Kit (Drop: Cerber)	261,851	application/x-msdownload

Figure 2. Another variety of PseudoDarkleech directs visitors to a redirect server, which will direct them to a RIG exploit kit

Two older malvertisement campaigns also use Cerber 4.0. One campaign employs the Magnitude exploit kit, which is a long time carrier of Cerber. Magnitude upgraded on October 3 and is continuously pushing Cerber 4.0 into countries in Asia, specifically Taiwan, Korea, Hong Kong, Singapore and China.

The second campaign typically employs a casino-themed fake advertisement, and researchers previously found it delivering the Andromeda or Betabot (detected by Trend Micro as Neurevt) malware to many countries. On October 4, Trend Micro researchers saw the campaign change their payload to Cerber 4.0 as well. This was the first instance that we detected it delivering Cerber 4.0, and it used the RIG exploit kit—another exploit kit that has a previous history with Cerber.

#	Result	Protocol	Host	URL	Comments	Body	Content-Type
1	200	HTTP	[redacted]	/?utm_source=cpm&utm_medium=pop&utm_campaign=redirect	"Casino" Malvertising	2,401	text/html
7	200	HTTP		/feed/stat.php	"Casino" Malvertising	348	application/javascript; charset=utf-8
24	200	HTTP	iz0cl.t55efnl.top	/?xniKfredKB3PA4c=l3SKfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-ofSih17OIFxzsqAycFUKCqr...	Rig Exploit Kit	2,217	text/html
25	200	HTTP	iz0cl.t55efnl.top	/index.php?xniKfredKB3PA4c=l3SMfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-ofSih17OIFxzsq...	Rig Exploit Kit	25,404	application/x-shockwave-flash
26	200	HTTP	iz0cl.t55efnl.top	/index.php?xniKfredKB3PA4c=l3SMfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-ofSih17OIFxzsq...	Rig Exploit Kit	25,404	application/x-shockwave-flash
29	200	HTTP	iz0cl.t55efnl.top	/index.php?xniKfredKB3PA4c=l3SMfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-ofSih17OIFxzsq...	Rig Exploit Kit (Drop: Cerber)	237,758	application/x-msdownload

Figure 3. RIG exploit kit malversting delivers new Cerber ransomware

Figure 4. The casino-themed fake advertisement

Neutrino exploit kit still live, now with Cerber 4.0

A new malvertisement campaign we first identified on September 8 was found distributing Cerber 3.0, before it upgraded to Cerber 4.0 on October 3. It was distributed to the US, Germany, Spain, Taiwan and Korea. Interestingly, the campaign used the Neutrino exploit kit to deliver this ransomware, despite claims by the Neutrino team that they stopped their service. Security researcher Kafeine reported a message from the Neutrino account on September 9: "we are closed, no new rents, no extends more". Though it appears that Neutrino has retreated; one speculation is that the crew is afraid of being exposed by cybersecurity firms. Another theory is that they have gone into "private" mode, meaning the exploit kit is only available for VIP clients handling larger operations.

#	Result	Protocol	Host	URL	Comments	Body	Content-Type
1	200	HTTP	[redacted]	/?utm_source=exo&utm_medium=cpm&utm_campaign=TWN&utm_content=popunder&site_id=238197	Fake AD	2,257	text/html
6	200	HTTP	billgory.xyz	/breeze.js	"NeutrAds" Malvertising	6,224	text/html
32	200	HTTP	billgory.xyz	/serene/karate/483461/deterrer/filmier/taping/parley/datively/clang.png	"NeutrAds" Malvertising	31	text/html
42	200	HTTP	billgory.xyz	/innateness/pleaters/moderatorship/equinity/italicize/distensibility/aviatrix/discomposure.asp	"NeutrAds" Malvertising	127	text/html
50	200	HTTP	cldlgw.middaymean.top	/pace/title-anywhere-17955517	Neutrino Exploit Kit	1,157	text/html
54	200	HTTP	cldlgw.middaymean.top	/peep/cGFpc3lhc3lxdA.swf	Neutrino Exploit Kit	71,078	application/x-shockwave-flash
64	200	HTTP	cldlgw.middaymean.top	/2010/05/16/struggle/distinct/aunt/kingdom-wide-suit-trouble.html	Neutrino Exploit Kit	31	text/html
67	200	HTTP	cldlgw.middaymean.top	/amongst/ZWZlcWx1Yw	Neutrino Exploit Kit (Drop: Cerber)	227,501	application/octet-stream

Figure 5. Neutrino malvertising serves Cerber ransomware

Solutions and Mitigation Tactics

Ransomware is an evolving threat, and the most fundamental defense is having proper backup processes in place. Follow the 1-2-3 rule: 3 copies, 2 devices, and 1 stored in a secure location. Data loss is manageable as long as regular backups are maintained.

Malvertising and exploit kits in general are being developed and improved constantly by cybercriminals, so keeping software updated with the latest security patches is critical for users and enterprises. This includes both the operating system and all applications being used. Make sure there is a security system in place that can proactively provide a comprehensive defense against attackers targeting new vulnerabilities.

Trend Micro offers gateway, endpoint, network, and even server solutions that protect enterprises and consumers.

PROTECTION FOR ENTERPRISES

- **Email and Gateway Protection**

  Trend Micro Cloud App Security, Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security addresses 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

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

Related Posts:

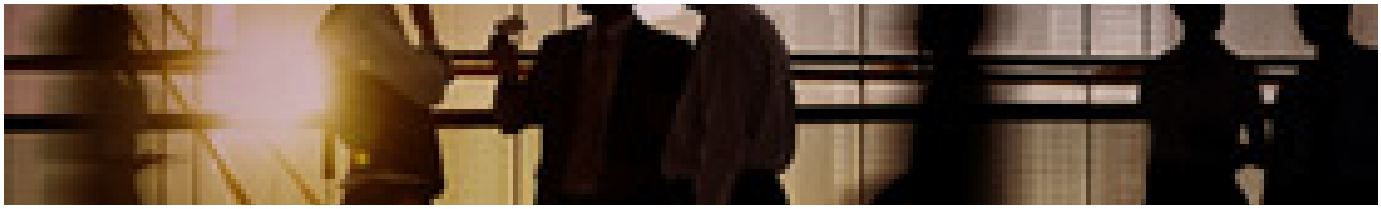
- **New Version of Cerber Ransomware Distributed via Malvertising**
- **CERBER: Crypto-ransomware that Speaks, Sold in Russian Underground**
- **Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit**
- **Cerber: A Case in Point of Ransomware Leveraging Cloud Platforms**

Tags: CERBERexploit kitsransomware

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

The Last Key on The Ring – Server Solutions to Ransomware

SEVERAL EXPLOIT KITS NOW DELIVER CERBER 4.0

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

Recent Posts

- The Last Key on The Ring – Server Solutions to Ransomware
- A Look at the BIND Vulnerability: CVE-2016-2776
- October Patch Tuesday: Microsoft Releases 10 Security Bulletins, Five Rated Critical
- Several Exploit Kits Now Deliver Cerber 4.0
- Funding Cybercrime: The Hidden Side of Online Gaming Currency Selling

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

DressCode and its Potential Impact for Enterprises
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Several Exploit Kits Now Deliver Cerber 4.0
Cybercriminals Improve Android Malware Stealth Routines with OBAD
BkSoD by Ransomware: HDDCryptor Uses Commercial Tools to Encrypt Network Shares and Lock HDDs

Latest Tweets

- How do cybercriminals abuse MMORPG currency systems to launder money and fuel malicious pursuits?… twitter.com/i/web/status/7…
  about 4 hours ago
- We've seen cybercrimes in movies like Jason Bourne and IT. Can those attacks happen in real life?… twitter.com/i/web/status/7…
  about 12 hours ago
- Think an e-mail attachment or link is suspicious? Verify first before responding. #ransomware

  about 15 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe