

CryptoLocker threats on the rise - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cryptolocker-threats-are-increasing>

Details:

Summary

This blog post, "CryptoLocker threats on the rise", is a blueAPACHE article from 2014 covering security. Over the last few weeks there has been a new episode in the on-going saga between the banking system and the Zeus and Cryptolocker families of malware. It is written for readers evaluating Managed Detection and Response, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2014
Topic	CryptoLocker threats on the rise
Services referenced	Managed Detection and Response, emPOWER Core Network & DC Interconnect, emPOWER Security
Named products or vendors	Windows, Palo Alto Networks

Article

Over the last few weeks there has been a new episode in the on-going saga between the banking system and the Zeus and Cryptolocker families of malware. The UK National Crime Agency issued an unprecedented warning over GOZeUS and CryptoLocker PC malware , which has already enabled cyber criminals to steal hundreds of millions of pounds through the theft of bank login credentials. A similar alert was raised in the US by the US-Cert . GameOver Zeus (GOZ) is a bank credential-stealing malware first identified in 2011 that has plagued the banking industry since then. It's often used by cybercriminals to target Windows based personal computers and web servers and carry out command-control attacks. Like many malware families today, Zeus and Cryptolocker utilise various Domain Generation Algorithms (DGA) to reach out to their command and control servers via DNS to establish contact and receive instructions. There are up to 1,000 domains per day that these families may reach out to. This can be one of the crucial breadcrumbs that help companies like Palo Alto detect them. As part of the proactive takedown initiated by the FBI in 2014, Palo Alto Networks and other companies, received intelligence that included about 250,000 URLs that P2PZeus and Cryptolocker will reach out to for the next 3 years. John Harrison, the Palo Alto threat prevention expert, has provided a list of best practices to ensure optimum and continuous protection from the "Crypto" and "Zeus" families, which respectively include Cryptolocker, CryptoDefense, or Cryptowall and P2PZeus, Zbot, GameOverZeus or GOZ, and may continue to resurface as other, as yet undefined versions. Note that

these best practices are applicable to many of malware families. These best practices include:

Use IPS signatures to prevent vulnerabilities from being exploited by client-side attacks that could drop Zeus or Cryptolocker.

Use Palo Alto Networks AV signature coverage for Cryptolocker and Zbot. Cryptolocker can come via social engineering through PDFs/Office documents or ZIP attachments that include malicious files.

Ensure DNS detection is enabled. Spyware and Command and Control detection will find infected systems that may pull down additional variants.

Utilise URL Filtering to prevent threats from being downloaded from malicious domains.

Turn-on Wildfire as it can detect unknown and zero-day malware or dropper related to Cryptolocker or Zeus.

Leverage file blocking – consider blocking all PE files or use a 'continue page' as an explicit warning to employees if they are allowed to download executable.

Decrypt from webmail – if an employee downloads a Fedex.ZIP that turns out to be Cryptolocker, make sure it gets inspected with threat prevention.

Track down and identify already infected systems – leverage the Botnet report provided by Palo Alto Networks to ensure that you haven't missed already infected systems.

Create a Sinkhole to systematical find infected systems – beyond the Botnet report, use this PAN-OS 6.0 feature to ensure that you are finding already infected systems easily.

Leverage firewall alert systems – investigate ALL TCP-unknown and UDP — unknown alerts. These could be the Command and Control vector for the malware or remote access trojan beaconing out.

Control your software update process – malware authors prey on social engineering tactics to get your employees to install fake Reader, Flash and Java updates – but these can be part of the infection vector. It's important that you recommend that employees do not install Adobe Reader, Flash and Java updates from unofficial sources if these pop-up. You might consider having all update installs controlled by the IT group or to explicitly direct users to visit the official software vendor website for updates.

blueAPACHE and Palo Alto work together to provide our clients with support and server or cloud protection against malware threats including CryptoLocker and GameOver Zeus. For more information on this article, visit the original post at Palo Alto here . For details on how to implement these best practices (and ensure you are protected by Palo Alto new generation firewalls), contact the blueAPACHE account team here .

Related

Managed Detection and Response

emPOWER Security (pillar hub)

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

emPOWER Security

Frequently asked questions

What two malware families does this 2014 article discuss?

Zeus (specifically GameOver Zeus, or GOZ) and Cryptolocker, described as being in an "on-going saga" with the banking system at the time of writing.

When was GameOver Zeus first identified, and what does it target?

GameOver Zeus was first identified in 2011. It is a bank credential-stealing malware often used to target Windows-based personal computers and web servers and carry out command-control attacks.

How many domains per day might the Zeus and Cryptolocker families contact?

The article states these families may reach out to up to 1,000 domains per day via Domain Generation Algorithms (DGA), which can be a crucial signal helping vendors like Palo Alto detect them.

How many URLs did Palo Alto Networks and other companies receive intelligence on as part of the FBI's 2014 takedown?

About 250,000 URLs that P2PZeus and Cryptolocker would reach out to over the following three years, per intelligence shared as part of the proactive takedown initiated by the FBI in 2014.

Who provided the best-practice list referenced in this article?

John Harrison, described as the Palo Alto threat prevention expert, provided the list of best practices for protection from the "Crypto" and "Zeus" malware families.

What is a "Sinkhole" and why does the article recommend it?

A Sinkhole is described as a PAN-OS 6.0 feature used to systematically find infected systems, recommended in the article as one way to identify already-infected systems beyond the Botnet report.

What does the article say about employees installing software updates?

It warns that malware authors prey on social engineering to get employees to install fake Reader, Flash and Java updates, and recommends that update installs be controlled by the IT group or that users be directed to official vendor websites.

What partnership does blueAPACHE describe in relation to these threats?

The article states blueAPACHE and Palo Alto work together to provide clients with support and server or cloud protection against malware threats including CryptoLocker and GameOver Zeus.

Source

origin post (2014)

Knowledge Base

What warning did the UK National Crime Agency issue regarding malware?

The UK National Crime Agency issued an unprecedented warning over GOZeus and CryptoLocker PC malware, which has already enabled cyber criminals to steal hundreds of millions of pounds through the theft of bank login credentials.

Did any other country raise a similar alert about this malware?

Yes, a similar alert was raised in the US by the US-Cert regarding the same malware threats.

What is GameOver Zeus (GOZ) and when was it first identified?

GameOver Zeus (GOZ) is a bank credential-stealing malware first identified in 2011 that has plagued the banking industry since then. It's often used by cybercriminals to target Windows-based personal computers and web servers and carry out command-control attacks.

How do Zeus and Cryptolocker malware families communicate with their command and control servers?

Like many malware families, Zeus and Cryptolocker utilise various Domain Generation Algorithms (DGA) to reach out to their command and control servers via DNS to establish contact and receive instructions. There are up to 1,000 domains per day that these families may reach out to, which can be a crucial breadcrumb that helps companies like Palo Alto detect them.

What action did the FBI take in 2014 regarding this malware, and what intelligence resulted?

As part of a proactive takedown initiated by the FBI in 2014, Palo Alto Networks and other companies received intelligence that included about 250,000 URLs that P2PZeus and Cryptolocker would reach out to for the next 3 years.

Who provided the list of best practices for protecting against Crypto and Zeus malware families?

John Harrison, a Palo Alto threat prevention expert, provided a list of best practices to ensure optimum and continuous protection from the "Crypto" and "Zeus" malware families, which include Cryptolocker, CryptoDefense, Cryptowall, P2PZeus, Zbot, and GameOverZeus (GOZ).

What are some of the best practices listed for protecting against Cryptolocker and Zeus malware?

Best practices include: using IPS signatures to prevent client-side exploit vulnerabilities; using Palo Alto Networks AV signature coverage for Cryptolocker and Zbot; ensuring DNS detection is enabled; utilising URL Filtering to prevent malicious domain downloads; turning on Wildfire to detect unknown/zero-day malware; leveraging file blocking of PE files; decrypting webmail attachments for inspection; tracking down already infected systems via Botnet reports; creating a Sinkhole to find infected systems; leveraging firewall alert systems to investigate unknown TCP/UDP alerts; and controlling the software update process to avoid fake Reader, Flash, and Java update scams.

How do you help protect clients against CryptoLocker and GameOver Zeus?

We and Palo Alto work together to provide clients with support and server or cloud protection against malware threats including CryptoLocker and GameOver Zeus.

Where can readers find the original source and more information about implementing these malware protection best practices?

for more information, readers can visit the original post at Palo Alto's research center, and for details on implementing the best practices with Palo Alto next-generation firewalls, readers can contact our account team via the contact page.