CRYPTOWALL VERSION 3 SEQUEL:
AN ANALYSIS TO ONE OF THE MOST
LUCRATIVE RANSOMEWARE

CRYPTOWALL VERSION 4 THREAT

EXECUTIVE SUMMARY

The Cyber Threat Alliance (CTA), formed in September 2014, undertook a huge effort of pooling the Alliance's collective resources to track and analyze CryptoWall, a prominent ransomware discovered in 2014. CTA focused its research efforts on the third variant of CryptoWall (CW3), which began its initial infection in January 2015. The Alliance used the fruits of this intelligence to enhance protection against this threat within each member's individual products and to build awareness with the public community through the publication of the CryptoWall version 3 Threat Report[1] as well as the release of indicators of compromise (IOC) through GitHub.

With the initial success of uncovering and subsequent protection against CW3, CTA continued to monitor CryptoWall's activity to learn and understand the repercussions and reactions from the malware authors. Unsurprisingly, CryptoWall authors were not deterred with the publication of CW3 and sharing of associated IOCs but were determined to release a fourth variant of CryptoWall (CW4) to overcome known malicious characteristics of its predecessor.

Based on the analysis of CW4, CTA researchers found the refreshed malware had similar traits to its predecessor but differed sufficiently to attempt evasion and kept an otherwise similar infrastructure of operation and distribution. Thus the focus of this updated report is to study the prevalence and global impact of CW4 as compared to CW3. Readers interested in CryptoWall malware characteristics should refer to the CryptoWall version 3 Threat Report.

Key Highlights of CW4:

- 15 campaign code identifiers
- 7,194,840 attempted infections
- 36,118 confirmed victims
- Estimated US$18 million in damages

WHAT IS RANSOMWARE?

Ransomware is a type of malware that encrypts a victim's files and subsequently demands payment in return for the key that can decrypt said files. When ransomware is first installed on a victim's machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more. Personal files, such as photos and home movies, may hold sentimental value to the victim.

Once these files are identified, the malware will encrypt them using a key known only by the attackers. In order to acquire this key to decrypt these files, the victim must pay a ransom to the attackers, often in the form of electronic currency such as bitcoin. In the event a victim does not have backups of this data, and chooses not to pay the ransom, these files are unlikely to be recovered. Ransomware has been known to cause irreparable damage to both individual users and large corporations alike.

There is another variant of ransomware that blocks the usage of the device with the same goal of extracting payment from the victim. This behavior includes spawning multiple messages across the screen disrupting user application usage or inhibiting the normal boot process of the operating system with displaying a ransom message instead of a user login screen.

1. CryptoWall v3 Threat Report: http://cyberthreatalliance.org/cryptowall-report.pdf

1. PREVALENCE

1.1 TARGETED REGIONS

During the period from November 2015 to June 2016, CW4 had reached a total of 7.1 million attempted infections spread across the globe with the largest impact found in North America (Figure 1). The same result resonated in CW3 (Figure 2). The main contribution factor is the willingness of victims to pay the required ransom to avoid the loss of business continuity.

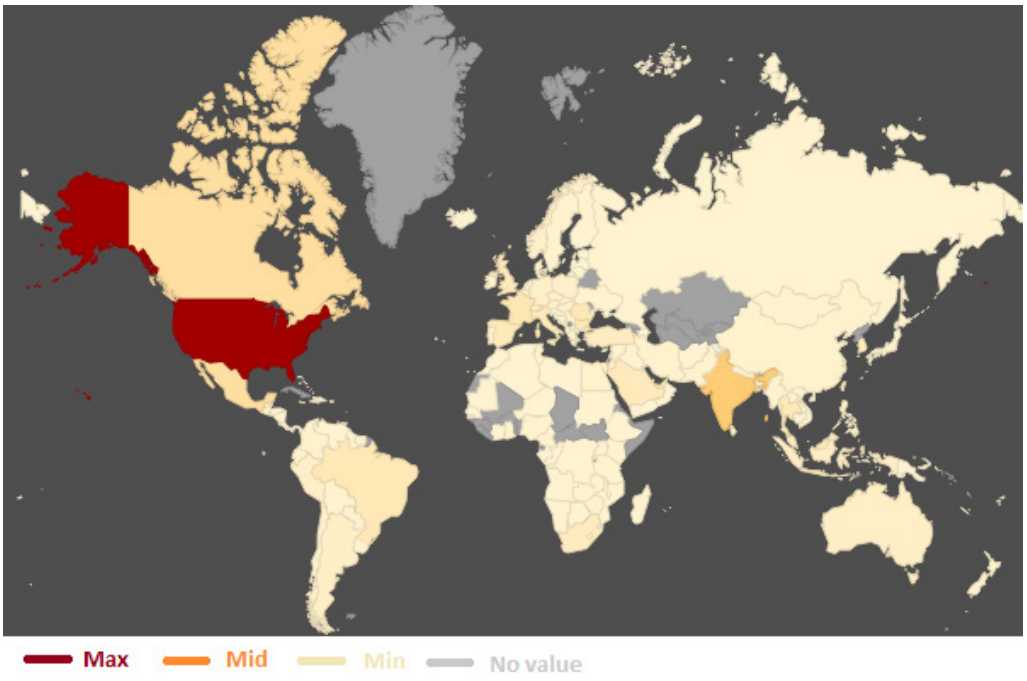

FIGURE 1 Heat Map of Attempted Infection of CW4

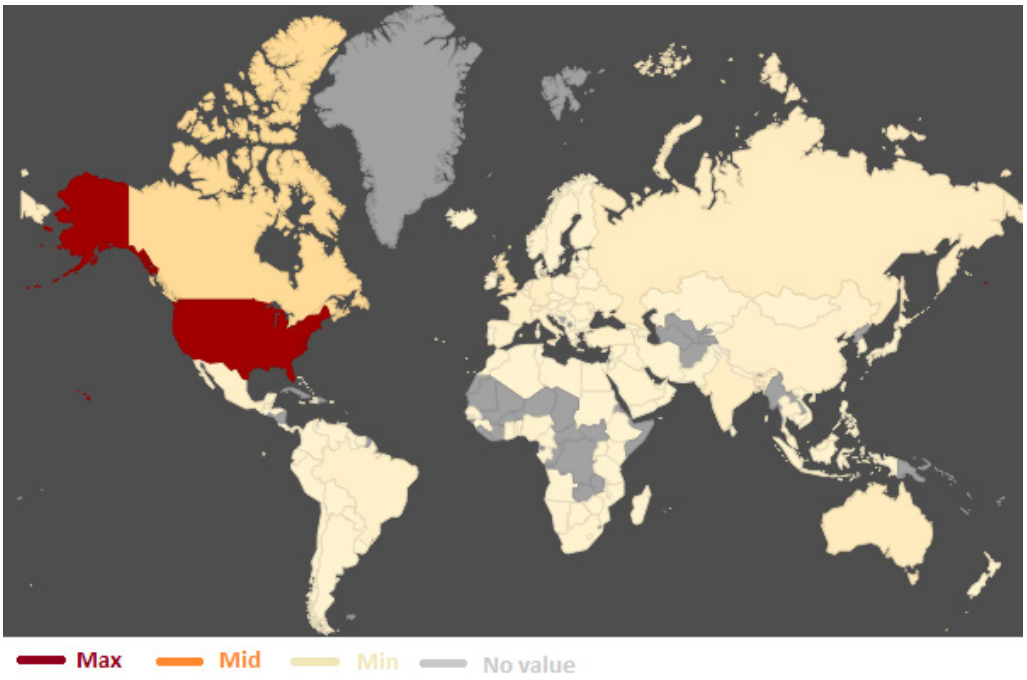

FIGURE 2 Heat Map of Attempted Infection of CW3

India is the second most-impacted country, the study found (Table 1). India's fast-growing IT industry typically supports multinational companies and operates mainly through the Internet. These factors have made them a significant target for CryptoWall as India rose from the bottom of the Top 10 in CW3 to the second in CW4.

CryptoWall v3	CryptoWall v4
United States	United States
Canada	India
United Kingdom	Canada
Australia	Mexico
Russia	United Arab Emirates
Germany	France
India	Romania
Italy	Taiwan
France	Jamaica
Netherlands	Bulgaria

TABLE 1 Comparison of Top Hit Countries

1.2 MALWARE TRACTION

During CW4's eight-month-long operation, CTA saw a total of 7,194,840 attempted infections with a peak of 228,496 in one day (Figure 3). This pales in comparison with CW3's 406,887 total attempted infections. Although CW4 was much more aggressive in its attempt to spread the malware (i.e., 18 times more than CW3), the number of confirmed victims was just 36,118. CW3, on the other hand, impacted hundreds of thousands of victims.

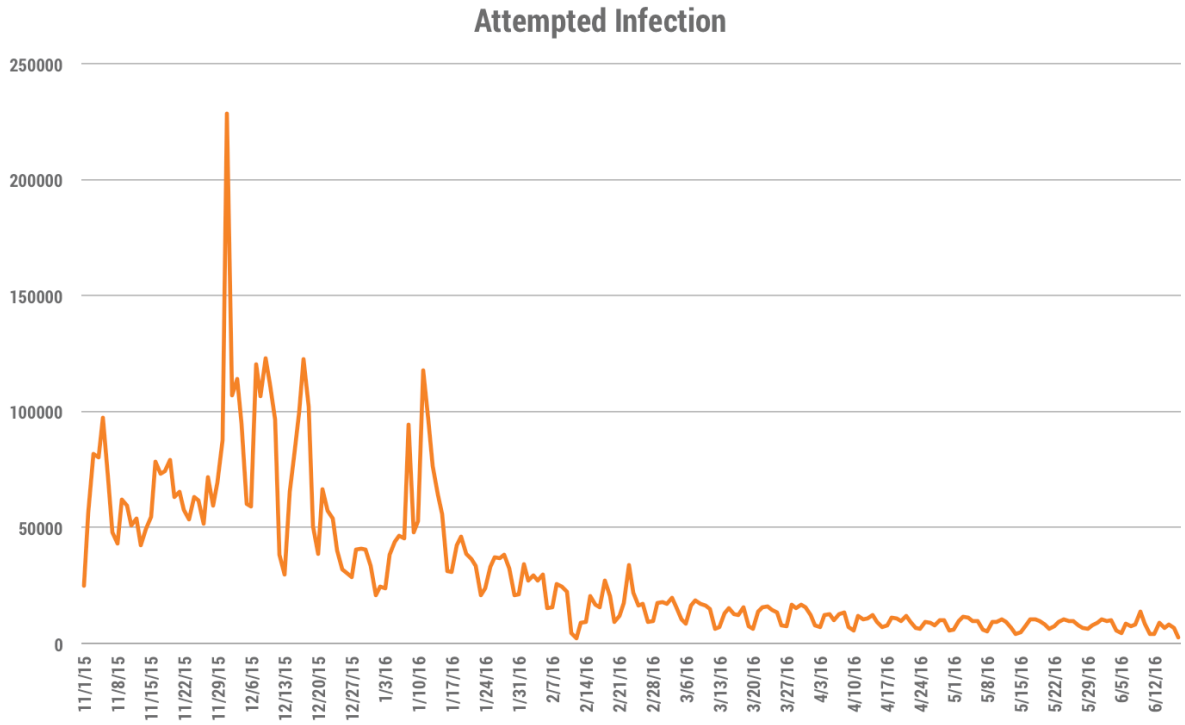

FIGURE 3 CryptoWall v4 Daily Activity

One could surmise that the promotion of awareness of CryptoWall and proactive protection provided to the public community served to dampen the success of CW4, leaving CW4 with a success rate of 0.5%. This is evidenced by a ratio of a much lower number of victims (Figure 4) in relation to the highest peak of attempted infections during the same active period. This impact led to two major consequences. First, a low success rate meant CW4 became less relevant as the usage (i.e., the number of attempted infections) dropped significantly after late January.

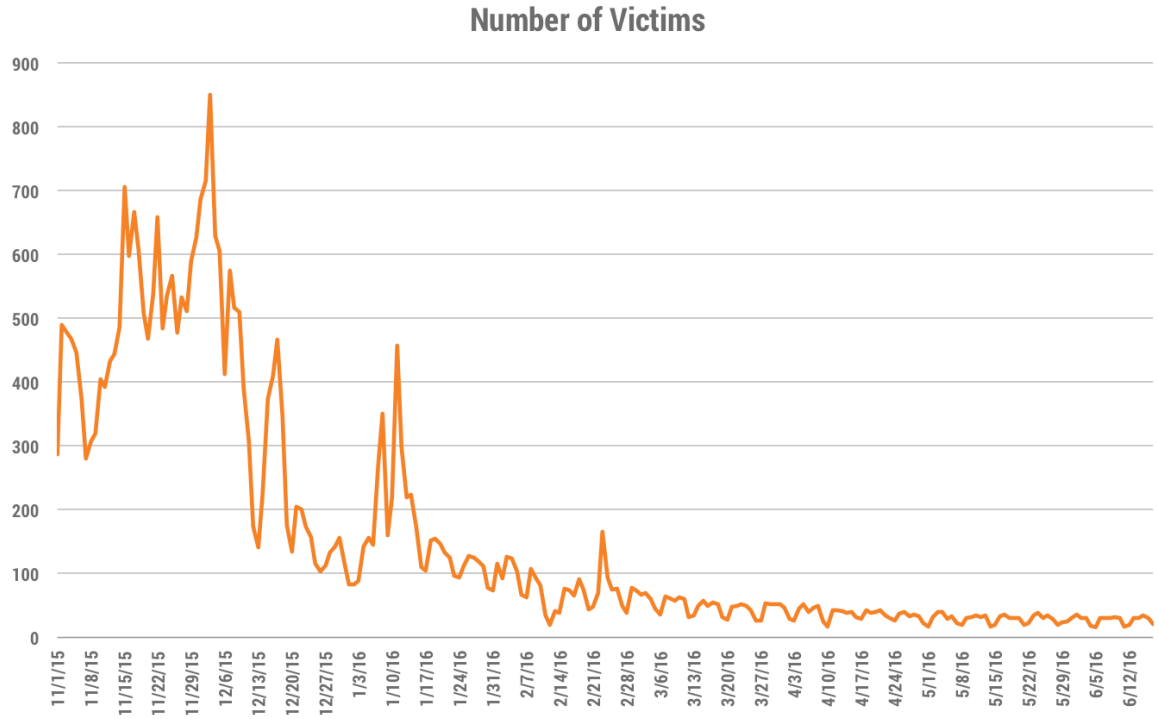

FIGURE 4 CryptoWall v4 Number of Victims

Since cyberattackers are opportunistic in nature, they quickly turn to other ransomware (Figure 5), rapidly transitioning to Locky and Cerber in the three-month window from February 19 to May 19, 2016.

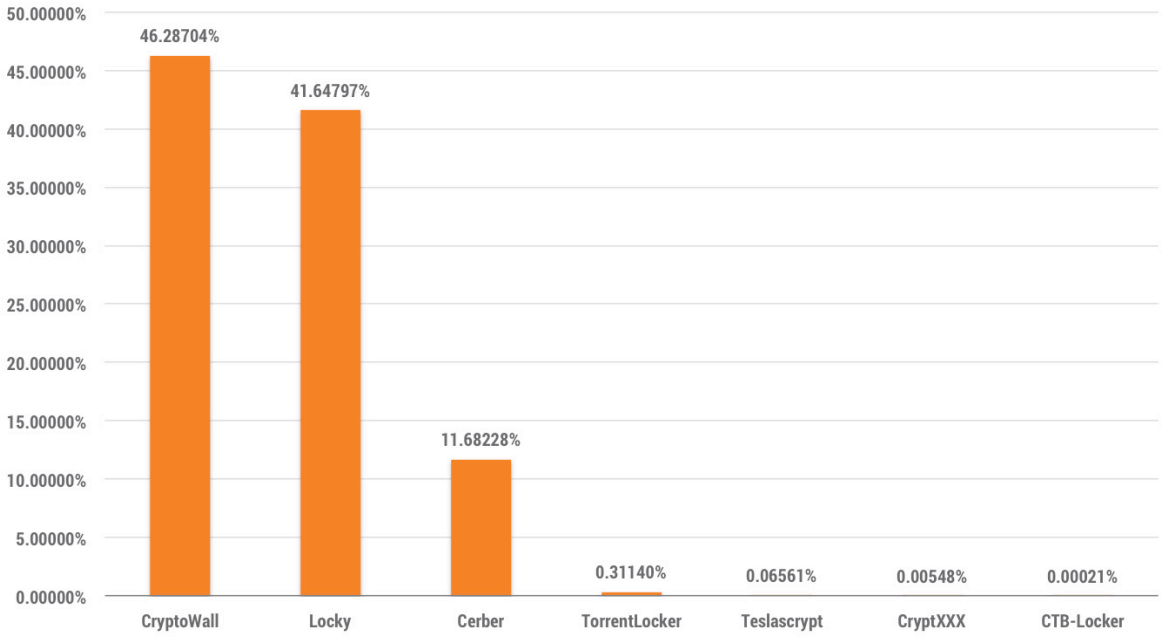

FIGURE 5 Ransomware Prevalence from February 19 to May 19, 2016

Second, a low success rate also meant a much lesser payout for CW4. Based on the average ransom price of $500 or 1 bitcoin, CTA estimates $18 million in damages associated with CW4 compared to $325 million with CW3.

THE PRICE OF RANSOM

The price paid by victims ranges from a few hundred dollars to over thousands of dollars (USD) based on the perceived value of the ransomed artifact(s). Payment responsiveness to a ransom affects the price ultimately paid (e.g., late payments could lead to as much as doubling of the asking price of the ransom).

2. PROPAGATION VECTORS

CTA researchers analyzed CW4 campaigns from May 19 to June 14, 2016 (Figure 6), and discovered "crypt7" was the most active campaign in CW4 as was in CW3. This indicates the same individual or group that was most active (i.e., 8,000+ sessions) and enjoyed past financial success with CW3 increased its investment by almost seven times on the fourth variant, reaching up to 55,170 sessions. Unfortunately, it did not pan out financially, as the total CW4 profit was estimated at $18 million when compared to CW3's profit of $325M.

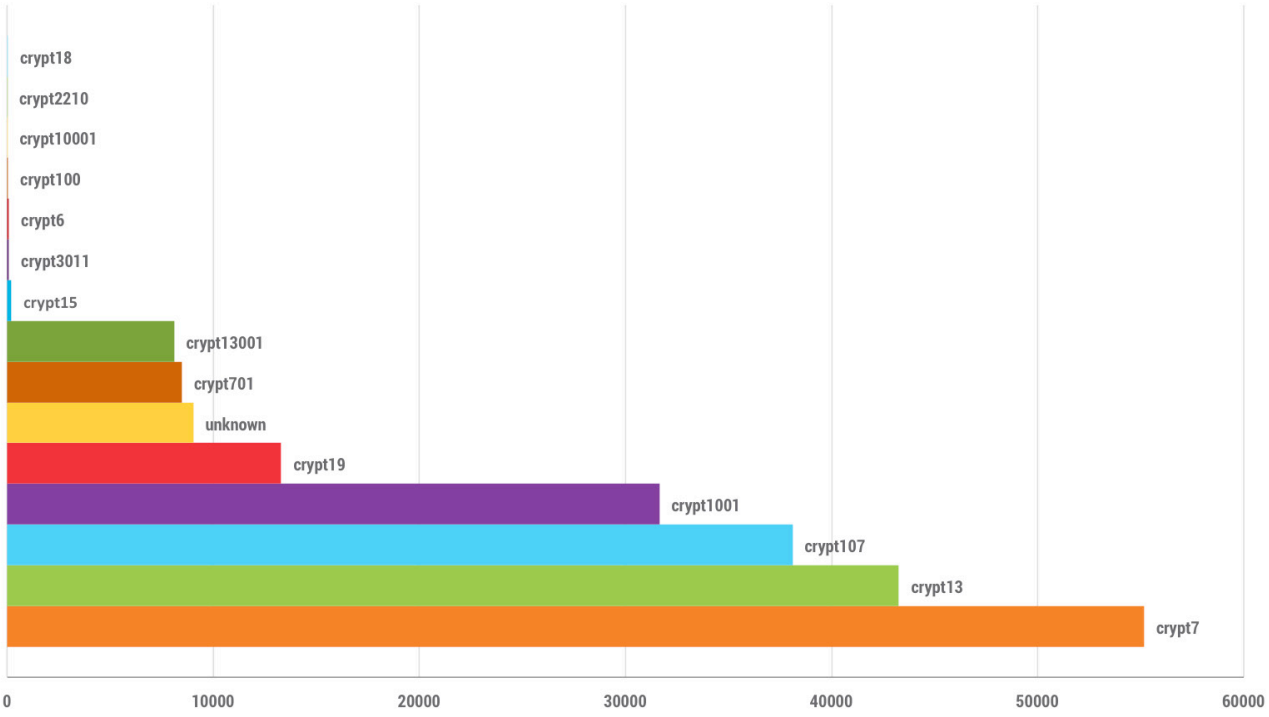

FIGURE 6 Top Campaign Identifier

CRYPTOWALL CAMPAIGN CRYPT ID CONVENTION

Campaign naming convention uses a string "crypt" followed by successions of numbers. This campaign identifier references the person or group that is attributed when successful infections are made. This attribution tracks the success of malware distribution and consequently the share of profit between cybercriminal organizations.

Both CW4 and CW3 campaigns follow the same malware distribution model (i.e., email phishing campaigns and exploit kits) (Table 2). Email phishing campaigns were the biggest contributor for CryptoWall distribution in both CW3 and CW4 campaigns due in part to user susceptibility to email as a vector of attack.

Propagation Vector	Campaign Identifiers
Magnitude Exploit Kit	crypt1001, crypt5022
Nuclear Exploit Kit	crypt19, crypt5022
Malicious Spam (Phishing)	crypt7,crypt1, crypt5022

TABLE 2 Propagation Vector and Campaign ID

CONCLUSION

The CryptoWall authors(s) mostly likely analyzed the flaws and characteristics of the malware published in the CryptoWall version 3 Threat Report. They showed persistence with the creation of the fourth variant of CryptoWall and characteristically held true to the tenacity of advanced cybercriminals. Fortunately, CW4 was materially less damaging at an estimated $18 million compared to CW3's $325 million, even though CW4 was more aggressive at 7.1 million attempted infections compared to CW3's 406,887 attempted infections. CW4's low success rate (i.e., 0.5%) eventually led to the decline of this malware activity after January 2016.

However, the waning of CW4 in the following months also saw a rise of Locky and Cerber ransomware. The flexibility tied to financial motivation of cybercriminals cannot be understated as they continue to prey on organizations concerned with business continuity such as those found in North America and many developed countries.

Email phishing continues to play an important role in distributing CryptoWall, thus malware protection for email should be a serious consideration for the reader.

This updated report on CryptoWall marks the Cyber Threat Alliance's second milestone since the release of the CryptoWall v3 Threat Report. The Cyber Threat Alliance and its members are dedicated to identifying, researching, and exposing incredibly dangerous and impactful threats around the world in order to better protect our customers and the open source community.

For more information on the Cyber Threat Alliance and how you can participate, please visit **http://cyberthreatalliance.org/**.

cyberthreatalliance.org

© September 2016 by the Cyber Threat Alliance Founding Companies. All Rights Reserved.

This document is intended for educational purposes only and may not apply to all situations. Professional advice should be sought before taking any action based on the information contained in this document. This document is subject to change without notice, however, the authors have no duty to update the information contained in this document and will not be liable for any failure to update such information.