DAMBALLA

State of Infections Report

Q2 2014

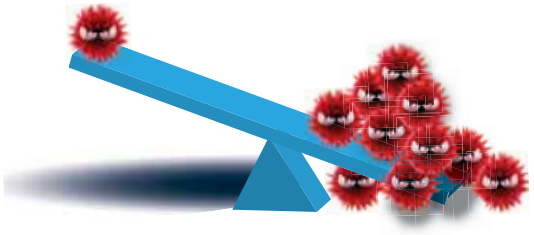
Table of Contents

Overview

The State of Infections in Q2 2014 were notable in two ways:

1. First, ransomware appeared nearly everywhere, grabbing international headlines and showing vigorous activity. Unlike traditional malware, which conducts its criminal activity in the background, ransomware is essentially a cyber stick-up. The victim is immediately locked out of their computer. Most will not regain control even if they pay the ransom demand.

2. In addition to ransomware run amok, Damballa also observed big swings in infection rates among enterprises large and small. The diversity of data serves as a reminder that organizations of every size must vigilantly defend against advanced threats.



Section 1: Mass Ransomware Infections Reach a Tipping Point

Ransomware on the Rise: The Quest for Easy Money

Cyber criminals are increasingly using ransomware in their quest for easy money. Unlike traditional malware, which relies on remaining stealthy while stealing data, ransomware is nothing short of a cyber stick-up. The malware takes your computer hostage, locks files, splashes fake legal warnings on the screen and tries to shock or shame you out of hundreds of dollars in ransom.

Damballa's Threat Research team noted a steady uptick in ransomware infections over the past 18 months, culminating during Q2 2014. Ransomware is popular because it provides criminals with a quick, low-risk pay-off. Malware authors can tally up to $1,000 per victim and ransom is paid via untraceable electronic currency.

Damballa Reports on Kovter Actvities:

43,713

At the height of Q2 activity Kovter infections reached 43,713 on a single day.

153%

Average daily infections increased a whopping 153% from April to May.

$1,000

Victims are prompted to pay up to $1,000 via credit card, but paying the ransom will NOT remove the malware or unlock your computer.

Kovter Ransomware Infections Skyrocket

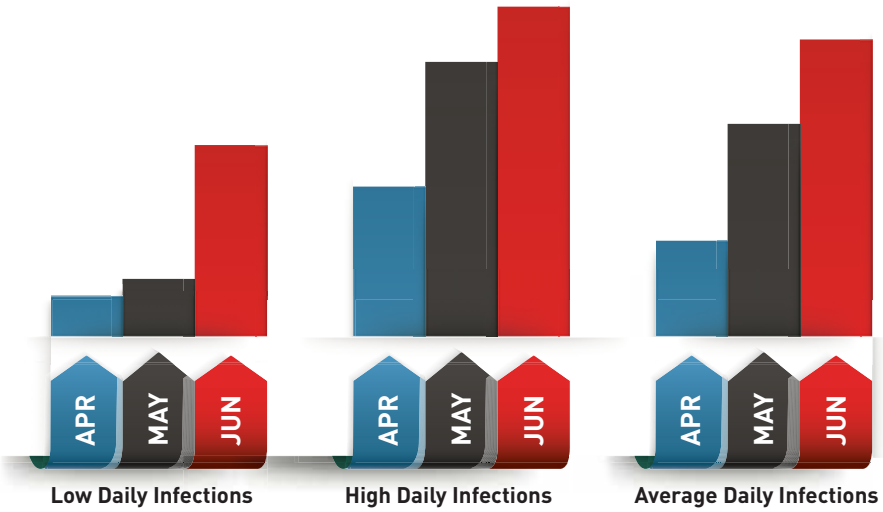
Kovter is a form of "Police Ransomware" first detected in 2013.

Kovter is a form of "Police Ransomware" first detected in 2013. It locks the computer, shows pornographic images and displays fake legal warnings.[1] Regardless of the victim's actual viewing history, the malware can present 'proof' of illicit activity and demand ransom to allegedly avoid penalties and jail time. It's essential for victims to know that paying the ransom will not remove Kovter from your system or restore its functionality.

Damballa saw a sharp rise in Kovter ransomware infections during Q2 2014. During the height of activity in June, infections reached 43,713 on a single day. Month over month, average daily infections increased a whopping 153% in May and 52% in June.

CHART 1: Average Daily Infections

Month	Daily Active Infection Counts LOW	Daily Active Infection Counts HIGH	Daily Active Infection Counts AVERAGE	Average Daily Increase vs Prior Month
April	6,602	18,089	9,783	70.61%
May	7,542	37,386	24,825	153.76%
June	25,852	43,713	37,733	52.00%



Low Daily Infections | High Daily Infections | Average Daily Infections

Ransomware Graphic

Click to view the Damballa Ransomware Infographic

Operation Tovar: Global Take-Down of CryptoLocker and GameOver Zeus

While Kovter thrived in Q2, the infamous CryptoLocker ransomware was dealt a crippling blow. On June 2, 2014 the Department of Justice (DOJ) announced Operation Tovar, a global take-down intended to dismantle the prolific GameOver Zeus (GoZ) botnet and its destructive payload CryptoLocker.[2] The far-reaching technical and legal operation involved the private sector, research community and law enforcement agencies in more than 10 countries. The primary objectives were to:

- Disrupt the GoZ distribution infrastructure
- Redirect victim computers away from Command and Control (C&C) servers to sinkholes
- Help victims remove GoZ infections from their computers

The DOJ estimates that CryptoLocker compromised more than 260,000 computers worldwide. About half of those infections occurred in the U.S and as many as 15,500 infections were in the U.K.[3] The FBI believes about $30 million in ransom was collected between September and December 2013. The GoZ botnet itself has infected more than one million devices globally and collected hundreds of millions of dollars through financial fraud.

Damballa Threat Research Team Contributes to CryptoLocker Sinkholing

CryptoLocker uses a sophisticated Domain Generation Algorithms (DGA) to evade security prevention controls. Damballa's threat research team began tracking CryptoLocker in October 2013 when the company's proprietary detection platform discovered its malicious activity before the malware was seen.

Later, the team obtained a sample of the malware and reverse-engineered it to decipher the algorithm. The intelligence was used to sinkhole all of the second level co.uk domains associated with CryptoLocker, which also used .biz, .com, .info, .net, .org and .ru domains.[4] The co.uk sinkhole recorded as many as 50,000 unique IPs per day.[4]

Resurgence of GoZ

Since Operation Tovar was announced, Damballa is often asked if GoZ has re-emerged. While the 'original' versions of GoZ and Cryptolocker haven't been resurrected, a new variant of GoZ, sporting a new DGA, has been spreading and trying to build up a new botnet.

This is to be expected. Threat actors are cunning human adversaries who can adapt. History tells us they will continue to upgrade, update and improve their malware. That doesn't mean we should give. When the opportunity exists to go after the bad guys, we must seize it.

A New Era in Cyber Public Health

Operation Tovar reflects the security community at its best. Stakeholders worldwide cooperated for the greater good of cyber public health. Whether the impact is temporary or not, we're learning important lessons. For instance, we know that a carefully orchestrated, far-reaching take-down should include:

- Global partnerships between public and private entities
- Criminal and civil legal processes designed to stop communications between infected computers
- Cooperation from domain registrars who agreed to block or sinkhole the DGA elements of the infections
- Mass notification of victims and easy access to malware removal kits

> "One thing is certain – managing mass cyber infections requires global cooperation and coordination."

We also know it's possible to make a dent in the machine that is the cyber underground. On July 11, 2014 the Justice Department reported there has been a 31 percent reduction in the number of computers infected with GoZ.[5] Additionally, they noted that CryptoLocker has been neutralized since it can no longer communicate with the GoZ C&C infrastructure.

While a single campaign won't permanently change criminal or end-user behavior, one thing is certain – managing mass cyber infections will become the norm in our interconnected world. Everyone has a stake in keeping the Internet safe, whether you're an individual user or a large enterprise with hundreds of thousands of users.

Section 2: Enterprise Infection Rates Vary Greatly

Number of Infections Doesn't Equate to Enterprise Size

As mentioned eariler in this report, traditional malware relies on remaining hidden so it can conduct criminal activity unimpeded. The longer it goes undetected, the more damage it can do. Hidden infections bedevil enterprises who spend a lot of money and manpower to prevent malware from entering their networks.

Infection rates vary greatly from enterprise-to-enterprise and from day-to-day. During Q2 2014, Damballa saw enterprises with 200,000+ devices experience only a handful of infections and those with under 600 devices have alarmingly high numbers of infections - and everywhere in between.

On any given day during Q2 2014, the ratio of active infected devices ranged from under .1% up to 18.5%. The following chart is an example of how the data can be extrapolated depending on the enterprise's size.

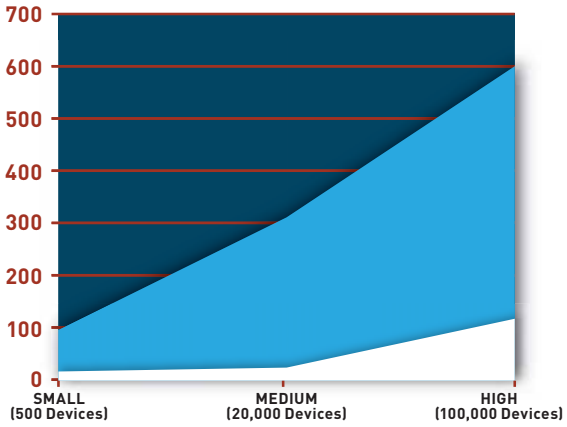


CHART 2: Example of Infection Rates

ENTERPRISE SIZE RANGE	LOW END: Infected Device Count @.1%	HIGH END: Infected Device Count @.18.5%
Small (500 Devices)	1	93
Medium (20,000 Devices)	20	3,700
High (100,000 Devices)	100	18,500

INFECTION vs. ALERT

It's important to note the difference between infections and alerts. Damballa finds actual **infections** - a status we assign to a device after we automatically compile proof that it is infected. An **alert** is an indicator that malicious activity may be present. Security teams must manually compile evidence from logs or forensics to prove an alert is an infection. Knowing with certainty that a device is infected speeds the time to remediation.

Another item of note is that infections are not active every single day. Advanced malware is designed to be evasive. It may stop communicating to its Command & Control server at any time. That's why it's critical to observe a device's activity over time to compile definitive of infections. If you rely on security prevention controls that only watch the attack vector, you can miss some criminal activity altogether.

Use Cases

The use cases below can help explain why infection ratios can vary greatly. For some enterprise security teams, even one infected device on their network poses too high of a risk. The ability to automatically detect actual infections and shorten the time to respond can prevent serious damage to the business.

1

Acme Company is a small enterprise with a high infection rate. Their distributed network is used by third-party contractors who primarily work outside of the corporate network. Acme Company's security team is challenged in a few ways:

- The company doesn't own the contractors' devices so they have less control. They can't necessarily push Anti-Virus updates or stop users from downloading executable files that may carry malware.
- Network security prevention tools can't detect infections unless they come through the front door. So if an infected agent device re-connects to the network, prevention controls would miss it entirely.

2

Beta Company is a large enterprise with a low infection rate. Their security team has tight controls in place, including:

- Denying administrative rights to general users
- Disallowing Internet browsing
- Disabling USB ports (thumb drives)
- Restricting inbound files
- Disabling email links

Conclusion

Cyber security issues effect every user on the Internet. Whether managing mass cyber infections like GoZ and CryptoLocker or infections within an enterprise, the work is daunting. Our adversaries are well-funded, agile, and adaptive. They constantly seek the next weakness to exploit. Our ability to automatically detect infections with certainty and speed the time to response can help prevent loss.

References

1. Kovter Ransomware Grows
2. U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "CryptoLocker" Ransomware, Charges Botnet Administrator, U.S. Department of Justice, June 2, 2014
3. Two-week opportunity for UK to reduce threat from powerful computer attack, National Crime Agency, June 2, 2014
4. What We Learned From Sinkholing CryptoLocker – Ushering in an Era of Cyber Public Health, June 2, 2014
5. Department of Justice Provides Update on GameOver Zeus and Cryptolocker Disruption , July

About Damballa

As the experts in advanced threat protection and containment, Damballa discovers active threats that bypass all security prevention layers. Damballa identifies evidence of malicious network traffic in real time, rapidly pinpointing the compromised devices that represent the highest risk to a business.

Our patented solutions leverage Big Data from the industry's broadest data set of consumer and

enterprise network traffic, combined with machine learning, to automatically discover and terminate criminal activity, stopping data theft, minimizing business disruption, and reducing the time to response and remediation. Damballa protects any device or OS including PCs, Macs, Unix, iOS, Android, and

embedded systems. Damballa protects more than 440 million endpoints globally at enterprises in

every major market and for the world's largest ISP and telecommunications providers.

To learn more about Damballa Failsafe visit our website www.damballa.com, contact us at 800.820.4527 or follow us on Twitter@DamballaInc.