

# The Reign of Ransomware: 2016 1H Security Roundup

Rami Naccache, *Systems Engineering Manager*  
Trend Micro North Africa

All your important files are encrypted!

But not just them... There are backups of all your files in a TB backup drive (encrypted).

To decrypt, you must send us this small (about 1MB) your personal code. (Don't provide code and you will receive a backup of your files. Total of 0.5 Btc).

After that during 4-5 days the software will send to you - Decryptor - and the necessary instructions. All charges in hardware configuration of your computer may make the decryption of your files absolutely impossible. Decryption of your files is possible only as you get recovery of backup during 7 days after which the program "Decryptor" will not be able to remove signature from the public source.

Time left: 60:4

**How much do you  
value your data?**

\$100?

\$500?

\$20,000?



# Threat Realities



## Ransomware

172% growth in  
6 months



## Ransomware

US\$ 209 Million  
ransom paid in  
(JAN – MAR  
2016)

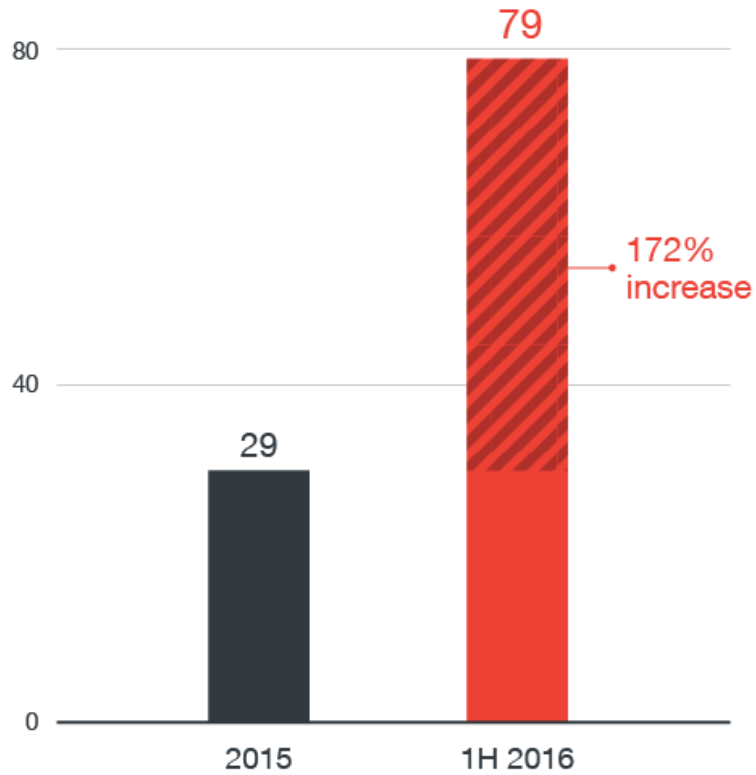


## BEC

US\$ 3 Billion  
lost globally  
(since JUN  
2016)





Ransomware is the  
biggest threat of 2016.



172% growth rate  
in the first 6  
months of 2016

# Industry Impact



## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**June 23, 2015**

Alert Number  
**I-062315-PSA**

### CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.<sup>1</sup> CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between \$200 and \$10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over \$18 million.



# New Ransomware Behaviors

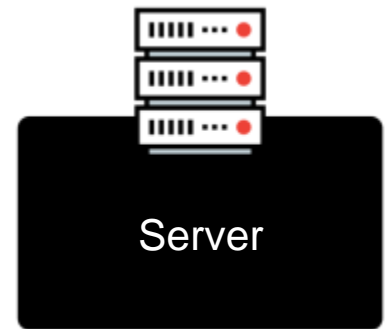
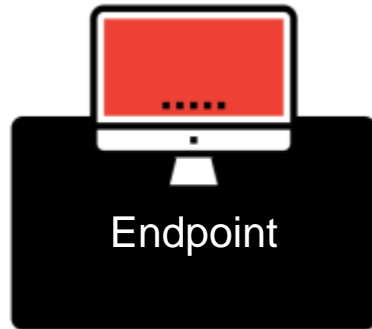
- Improved social engineering lures
- More platforms and systems to infect
- New network-related capabilities
- New extortion tactics
- Direct server attacks

# Ransomware Targeting Enterprise



Trend Micro multilayered  
defense addresses  
ransomware at any stage  
of infection.

# Ransomware Entry Points



Business Email  
Compromise threatens  
organizations globally.



- 1 Threat
- 22,000 victims worldwide
- US\$ 120,000 loss per scam
- \$3B worth of losses globally

# Most Affected Countries



# BEC Tactics

- Bogus invoice scheme
- CEO fraud
- Account compromise
- Attorney impersonation
- Data theft



# BEC Components



Social Engineering



Malware

Exploit Kits continue to make life difficult with new vulnerabilities and ransomware families.

# Exploit Kits and Vulnerabilities





1million hits to EK-  
hosting sites  
blocked monthly

473 vulnerabilities  
discovered in 1H

# Protection Against Exploit Kits



Trend Micro  
Virtual Patching



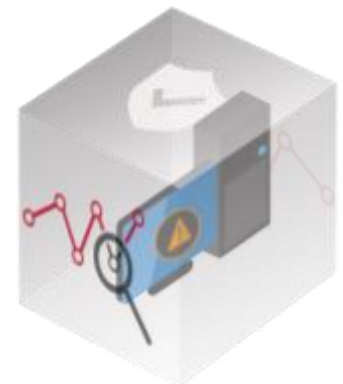
Trend Micro  
Deep Security



Trend Micro  
Vulnerability  
Protection



Trend Micro  
Network Defense



Digital Vaccine Labs

# The resilient threat of Data Breaches

# Recent 2016 Data Breaches



**360M** MySpace  
usernames and  
passwords



**464,000** unique  
social security  
numbers

# Prevention and Mitigation



Block or contain threat



Protect sensitive data



Point of Sale (PoS)  
malware hounding those  
behind the times



Payment systems are catching up to today's security needs.

But a majority still use traditional Point of Sale machines

For the complete report, please visit:

<http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-reign-of-ransomware>

Created by:

**TrendLabs**

The Global Technical Support & R&D Center of TREND MICRO