Global Internet Security Threat Landscape 2018

ITU Workshop on Advanced Cyber Security Attacks and Ransomware

Thomas Hemker, CISSP, CISM, CISA
Director Security Strategy, CTO Office - Symantec

Thomas Hemker, CISSP, CISM, CISA

23 Years IT-Security
PGP

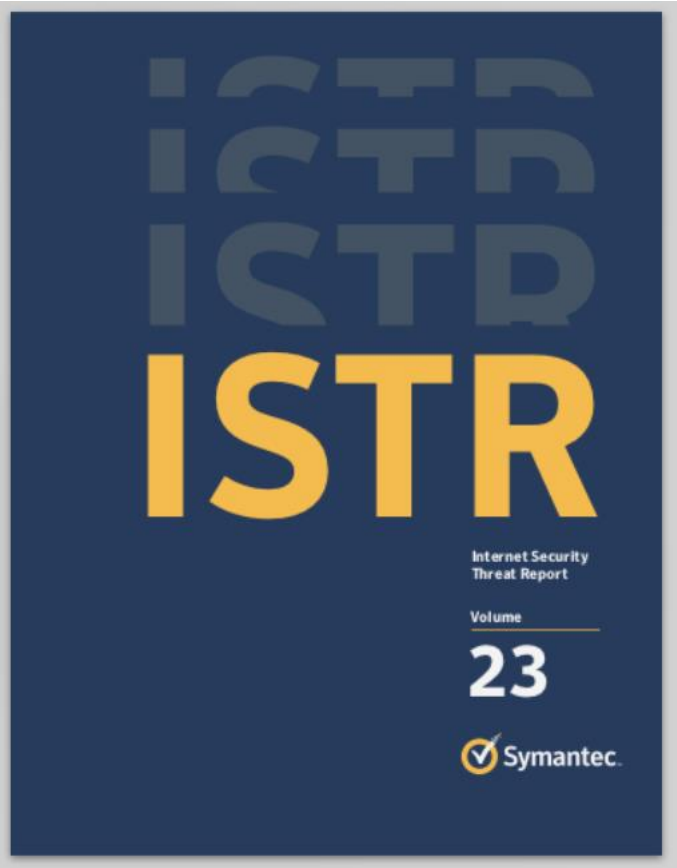
CTO Office
CISO Contactperson
Speaker, Author

ISF, TeleTrust, Bitkom, ENISA
ISACA, (ISC)2, HDG

Hamburg

#THeSecurity
(LinkedIn, XING, ResearchGate, noFB)

Thomas_Hemker@symantec.com

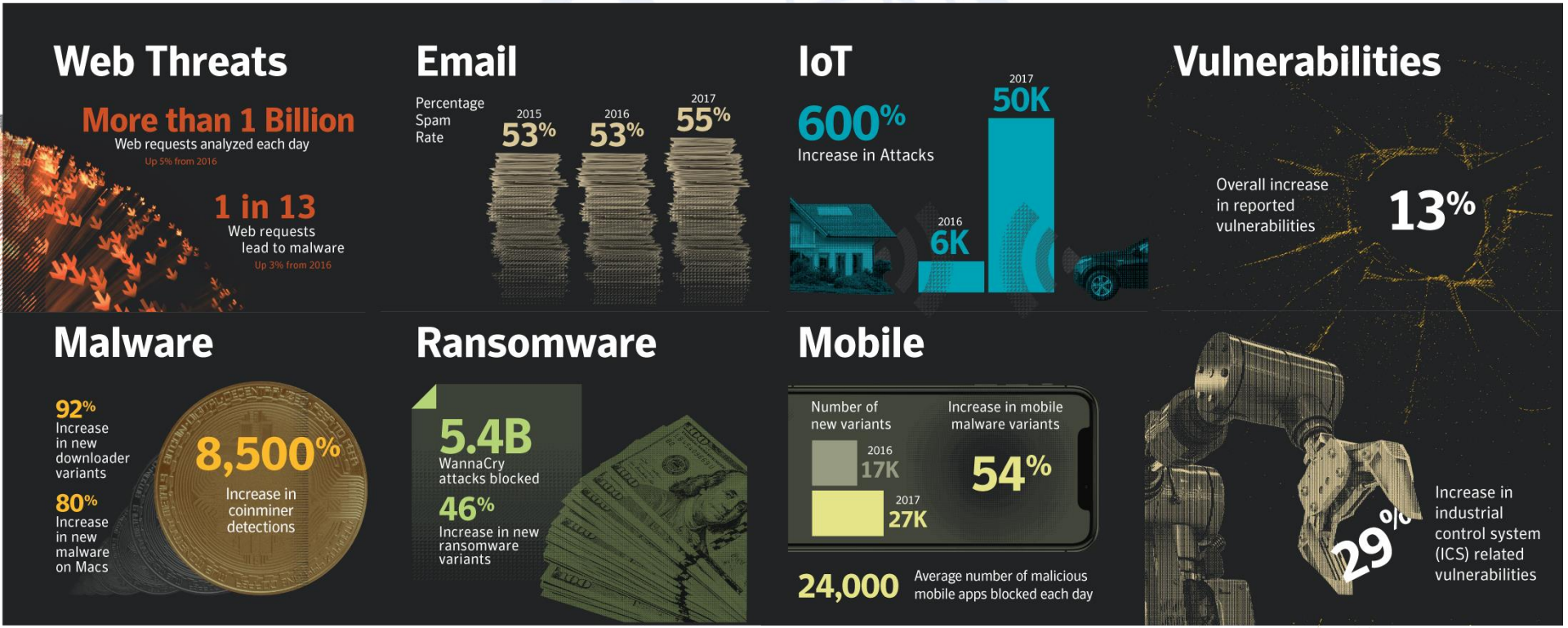


https://www.symantec.com/security-center
https://www.symantec.com/security_response/publications/monthlythreatreport.jsp
@threatintel

Threats


Negligent Employee
Other
Endpoints
Email
Network & Web
Spear-Phishing attacks
Advanced Malware
Spam
Malicious Websites
Ransomware

Big Numbers


Web Threats
More than 1 Billion
Web requests analyzed each day
Up 5% from 2016
1 in 13
Web requests lead to malware
Up 3% from 2016
Email
Percentage Spam Rate
2015 53%
2016 53%
2017 55%
IoT
600%
Increase in Attacks
2016 6K
2017 50K
Vulnerabilities
Overall increase in reported vulnerabilities
13%
Malware
92% Increase in new downloader variants
80% Increase in new malware on Macs
8,500%
Increase in coinminer detections
Ransomware
5.4B
WannaCry attacks blocked
46%
Increase in new ransomware variants
Mobile
Number of new variants
2016 17K
2017 27K
Increase in mobile malware variants
54%
24,000
Average number of malicious mobile apps blocked each day
29%
Increase in industrial control system (ICS) related vulnerabilities

Some Key Findings

- Cryptojacking Attacks Explode by 8,500 Percent
- Implanted Malware Grows by 200 Percent, Compromising Software Supply Chain
- Mobile Malware Continues to Surge
- Business-Savvy Cyber Criminals Price Ransomware for Profit
- Majority of Targeted Attackers Use Single Method to Infect Victims

Crypto Jacking Predictions

BOTNETS

Distributed mining, either through conventional botnets of malware-infected computers and IoT devices or browser-based coinminers, hosted on websites.

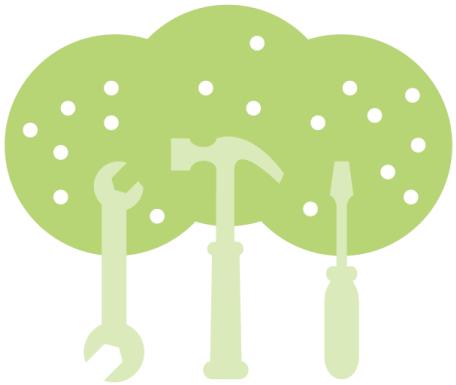
TARGETING ORGANIZATIONS

Targeting of corporate or organizational networks in order to harness the power of servers or supercomputers.

CLOUD HIJACKING

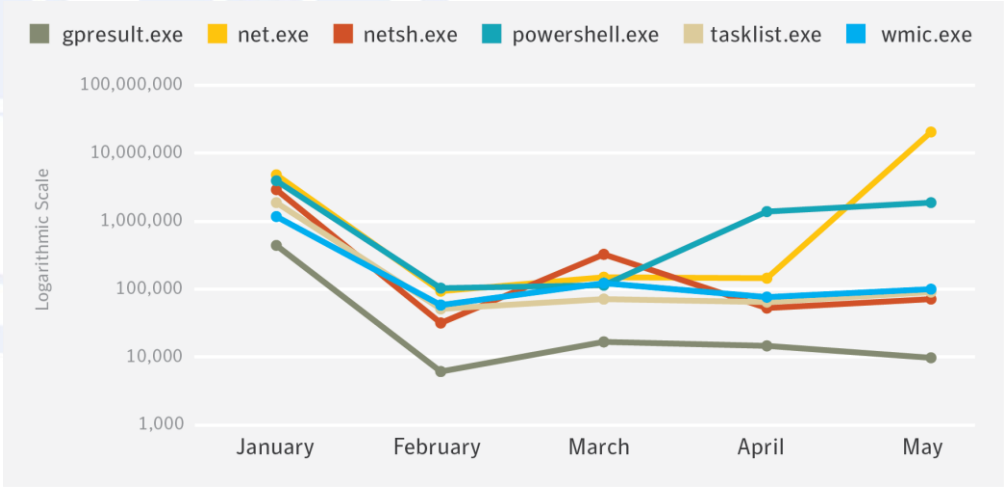
Cloud services offer the possibility of high-powered mining. This has a possible financial impact on cloud customers where they pay based on CPU usage.

Living off the Land



Definition: Living off the land

Only pre-installed software is used by the attacker and no additional binary executables are installed onto the system



Fileless Attacks
Memory Only Attacks
Dual- Use Tools
Targeted Attack Groups

Supply Chain Attacks

2015

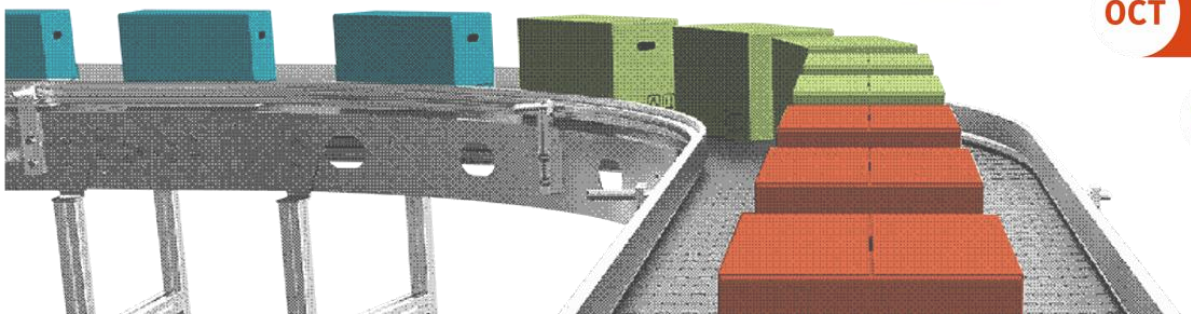
- APR: EvLog update compromised with malware
- MAY: Japanese Word Processor tool used to install malware
- JUN: XcodeGhost: Malware found in Apple dev environment
- DEC: Backdoor found in Juniper Networks firewall

2016

- SEP: S. Korean security software used to install malware
- OCT: Attackers hijack Brazilian Bank's entire DNS
- NOV: Ask Network Toolbar used to install malware
- DEC: Ask Partner Network updater used to install malware

2017

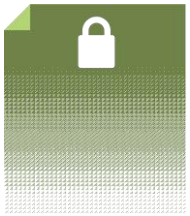
- FEB: • Trojanized version of Yeecall Pro for Android used to RAT • Kingslayer campaign hijacks sysadmin software updates
- MAR: Adobe reader installer bundled with malware
- MAY: • Handbrake video tool used to install malware • Operation WilySupply compromises editing tool updates
- JUN: M.E.Doc updater used to distribute Petya/NotPetya
- JUL: ePrica pharmacy software installs backdoor Trojan
- AUG: • CCleaner tool injected with malware • Backdoor found in NetSarang server mgmt. software
- SEP: • Modified Python modules found on official repository • "ExpensiveWall" malware found in Android SDK
- OCT: Elmedia Player for OSX bundled with malware
- NOV: Bitcoin Gold wallet replaced with malware
- DEC: Wordpress Plugins used to install Backdoors



Cybercrime Trends

Ransomware

Detections stable at 1,242 per day in 2017 (-2%)
Downloader detections increased by 92%
46% increase in new ransomware variants
Average ransom down to $522 from $1,070



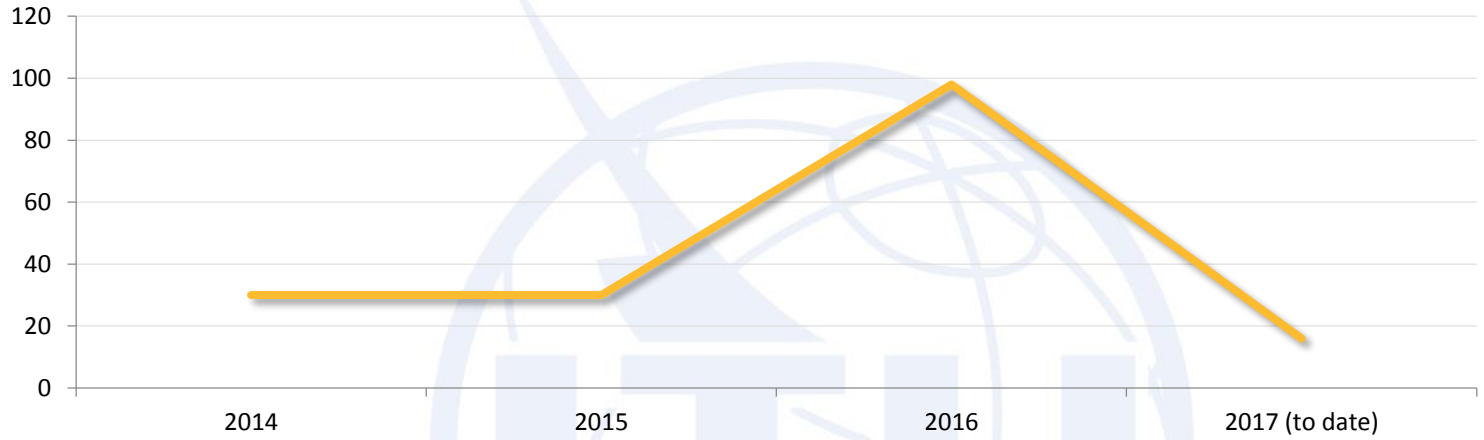
Shift to other attacks

To coin mining e.g. VenusLocker shifted from ransomware to crypto mining
To financial Trojans e.g. Emotet activity increased by 2,000% in Q4

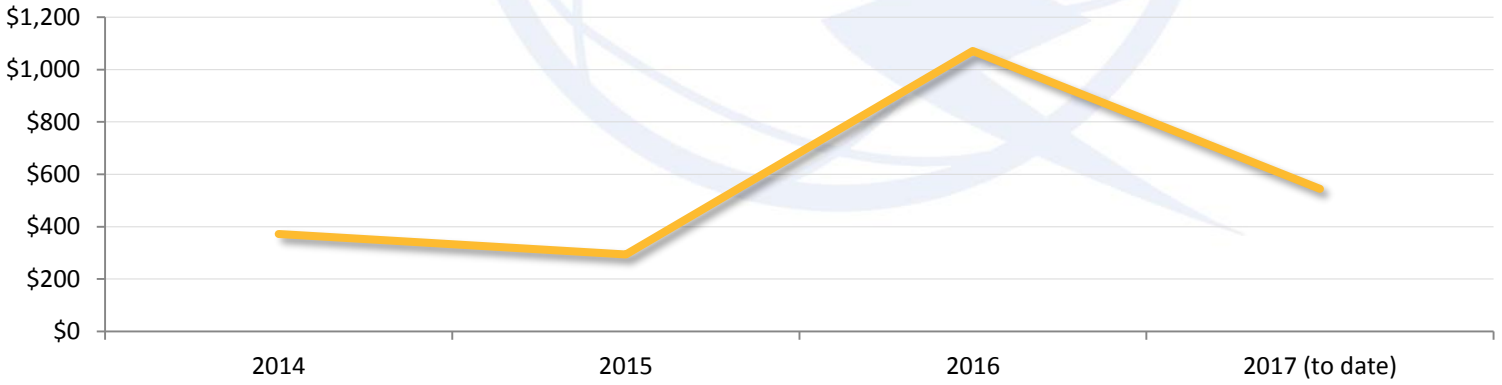
Ransomware

- The advent of worm-type ransomware is a new and highly disruptive avenue of attack
- Businesses in particular are most at risk to worm-type threats, which can spread in minutes across poorly secured networks
- Infection numbers are continuing to trend upwards, powered by the WannaCry and Petya outbreaks
- Average ransom appears to have stabilized at $544, indicating attackers may have found their “sweet spot”
- The U.S. is still the country most affected by ransomware, followed by Japan, Italy, India, Germany, Netherlands, UK, Australia, Russia, and Canada

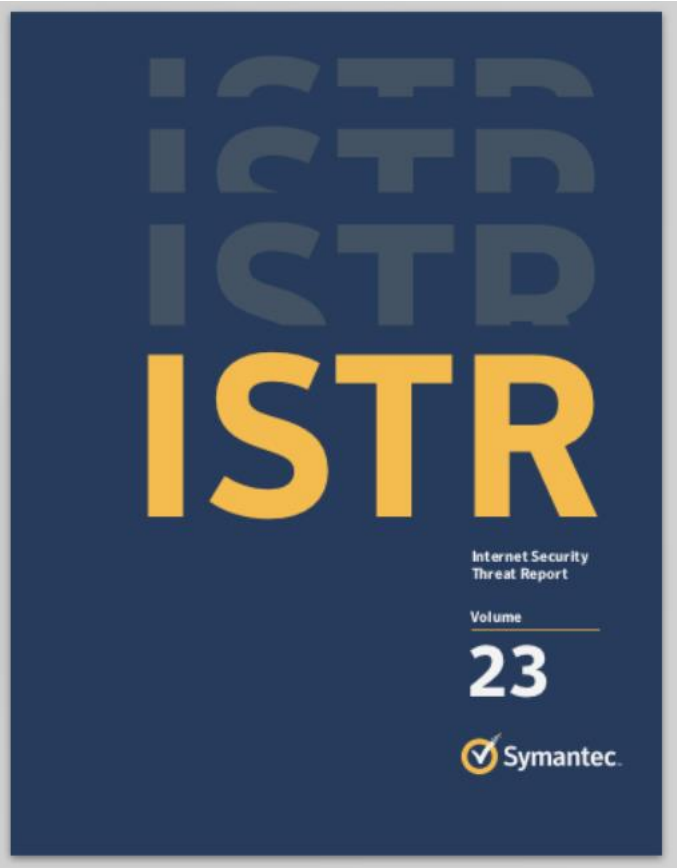
Families



Ransom



34% - 64%



https://www.symantec.com/security-center
https://www.symantec.com/security_response/publications/monthlythreatreport.jsp
@threatintel