1H’18 Security Roundup

Chris Jang

2018 Midyear Security Roundup

Unseen Threats, Imminent Losses

A review of the first half of 2018 shows a threat landscape that not only has constant and familiar features but also has morphing and uncharted facets: Ever-present threats steadily grew while emerging ones used stealth.

TREND MICRO

Vulnerabilities and Microprocessor Flaws

Firmware flaws and increased vulnerability advisories make patching an issue

Meltdown (CVE-2017-5754)

Affects every computing device using an Intel processor released since 1995

Spectre (CVE-2017-5753, CVE-2017-5715)

Affects computers and smartphones running x86 (Intel and AMD) and ARM-based processors

ZDI 1H’18 Results

602 reported vulnerabilities
23 published without patches

Vendor	2H 2017 vs. 1H 2018
Apple	92% increase
Foxit	50% increase
Adobe	7% increase

What enterprises are affected?

Best Practices Against Vulnerabilities

Regular and timely patching

Proactive measures such as vulnerability shielding

Compliance with protection and security regulations

Cryptocurrency mining and ransomware

Cryptocurrency mining detections increased and ransomware remains an enterprise threat

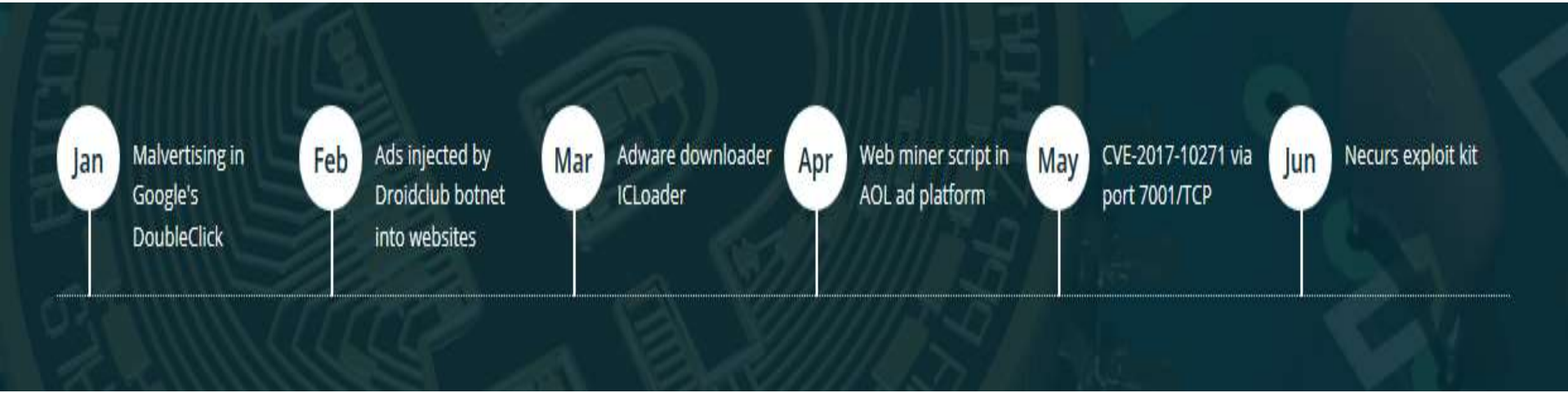
Cryptocurrency-mining detections

2H-2017	1H-2018
326,326	787,146

New cryptocurrency-mining malware families

2H-2017	1H-2018
3	47

Cryptocurrency mining attack methods seen



Best Practices for Crypto-Mining

- ✓ Regularly update devices with their latest firmware to prevent attackers from taking advantage of vulnerabilities to get into systems.
- ✓ Change devices' default credentials to avoid unauthorized access.
- ✓ Employ intrusion detection and prevention systems to deter malicious attempts.
- ✓ Be wary of known attack vectors, such as socially engineered links, attachments, and files from suspicious websites, dubious third-party applications, and unsolicited emails.
- ✓ Check systems for high resource utilization

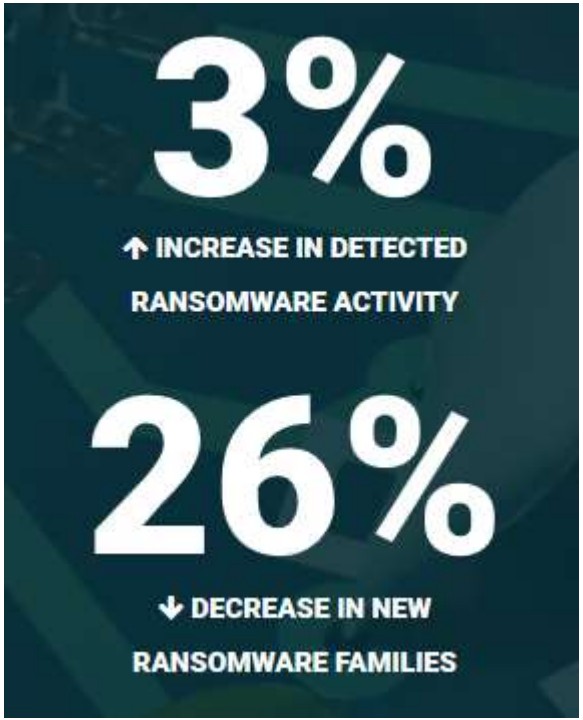
Ransomware 1H’18

Ransomware detections

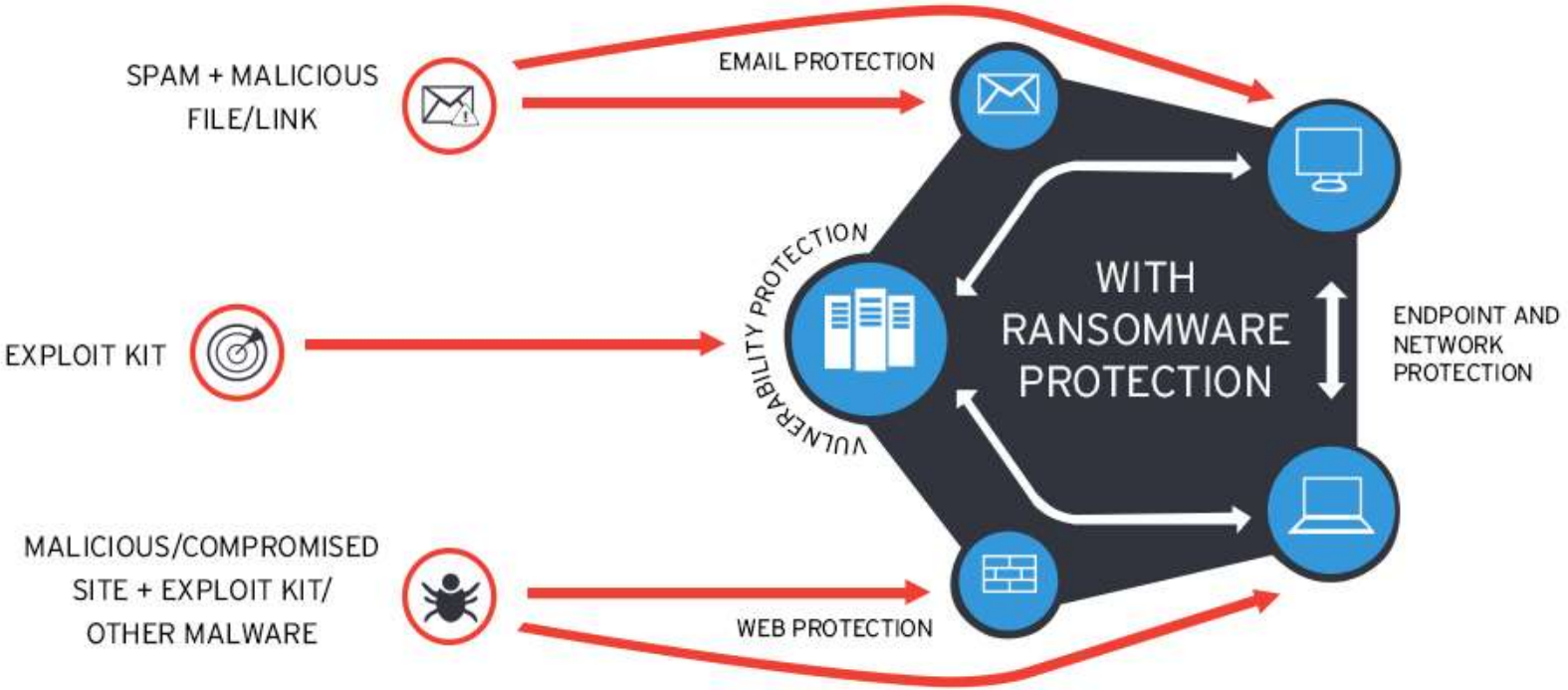
1H-2017	2H-2017	1H-2018
196,832	369,698	380,299

New ransomware families

2H-2017	1H-2018
159	118



Layered Protection Against Ransomware



Data breaches and regulatory issues

Costly data breaches continued to hit enterprises while governments increased regulations

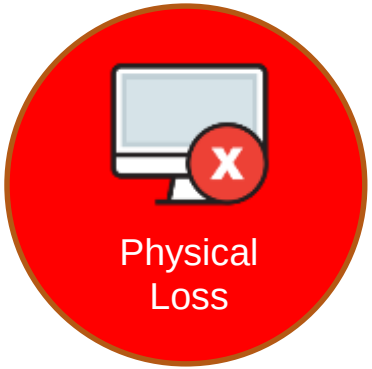
Reported data breaches in the US

2H-2017	1H-2018
224	259

Number of mega-breaches in the US

2H-2017	1H-2018
9	15

Source: https://www.privacyrights.org

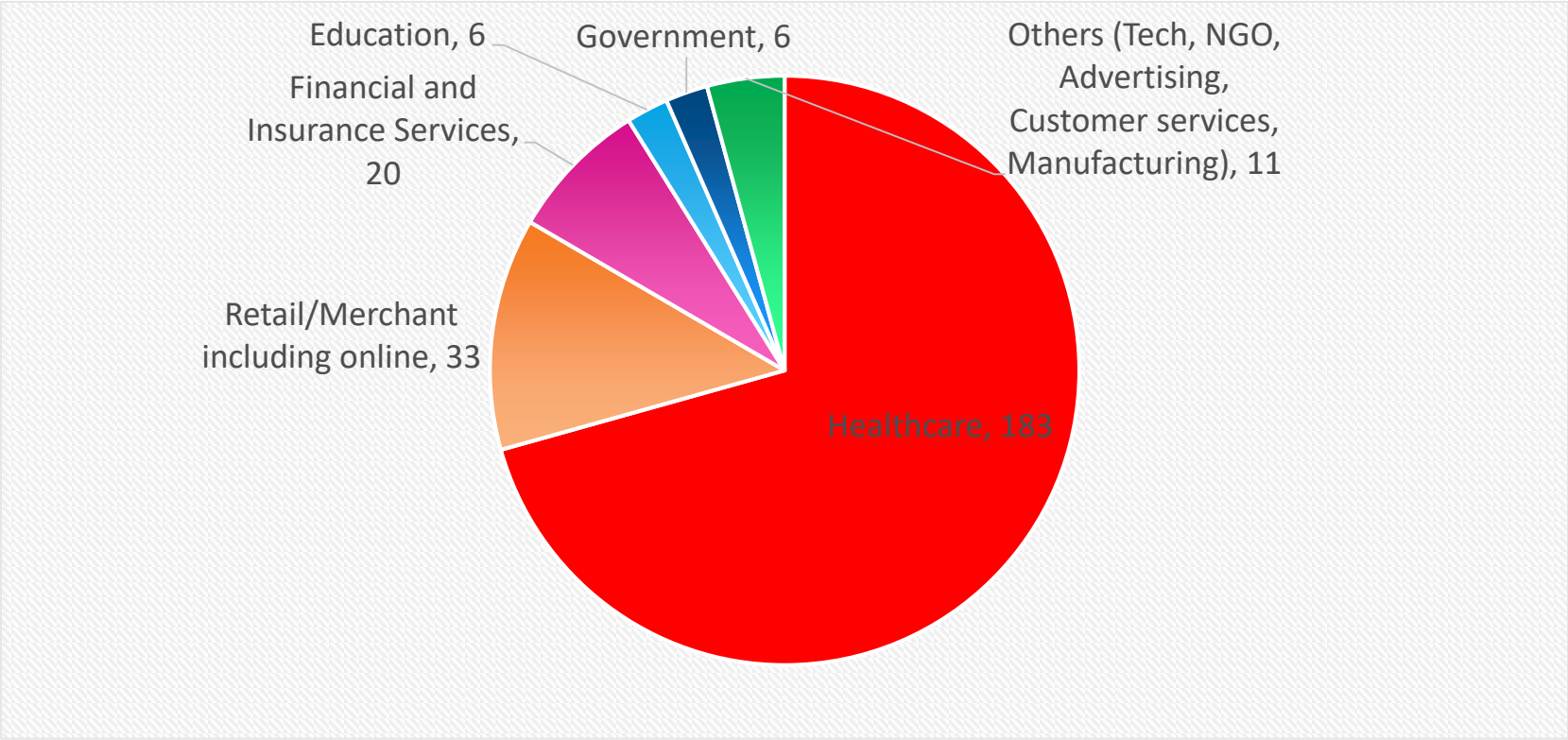


By Disclosure	42%
By Hacking	41%
Physical	16%
Insider and others	2%

Causes of Data Breaches in 1H-2018

Source: https://www.privacyrights.org

Most breached industries



Source: https://www.privacyrights.org

Best Practices Against Data Breaches

Classify high-value assets or core data.

Know the indicators of compromise (IoCs) of known attacks.

Secure all sections of the IT supply chain.

Patch and update systems regularly.

Comply with regulatory standards.

Fileless, Macro and Small-sized Malware

Cybercriminals tried to evade file-based detection

Small file size

Fileless malware

Malicious macros

Protection Against Malware Threats

Use endpoint application control and network-based solutions for POS malware

Integrate layered protection across the network to detect fileless threats.

Trend Micro uses non-file-based indicators like specific execution events or behaviors for tracking these threats.

Filter out attacks using the system's security settings, or avoid enabling macros for documents from new or unknown sources.

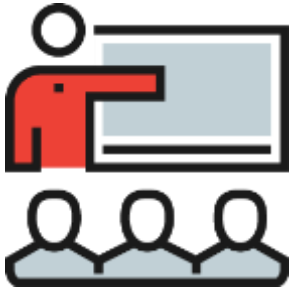
Business Email Compromise (BEC) scams

Losses from BEC scams exceeded projections and attempts increased

BEC Attempts Against Customers

2H-2017 BEC Attempts	1H-2018 BEC Attempts
6,533	6,878

Protection Against BEC Scams



Raise employee awareness on how the scheme works

Verify legitimacy of fund transfer requests

Verify supply requests and invoices from third parties

Smart Protection Network Data

Overall threats blocked in the first half of 2018

Smart Protection Network Data

Trend Micro

- 30 years focused on security software
- Headquartered in Japan, Tokyo Exchange Nikkei Index (4704)
- Annual sales over $1B US
- Customers include 45 of top 50 global corporations
- 6000 employees in over 50 countries

500k commercial customers &
250M+ endpoints protected

Market Leadership Position

IDC

The **market leader** in server security for **7 straight years**

Gartner

Trend Micro delivers **the most cloud security controls (16 of 21)** of all evaluated vendors.

- IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116
- Gartner "Market Guide for Cloud Workload Protection Platforms", Neil MacDonald, March 2, 2017

NSS LABS

Recommended Breach Detection System for **4 straight years**, and **Recommended** Next-generation IPS

Gartner

Leader in Gartner Magic Quadrant for Intrusion Detection and Prevention Systems, January 2018

- NSS Labs Breach Detection Test Results (2014-2017); NSS NGIPS Test Results, 2017
- *http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/*

Gartner

Named a Leader Once Again in the Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2018

AV-TEST

#1 in protection and performance

- *https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html*
- av-test.org (Jan 2014 to Dec 2017)