Fortinet Threat Report

Matteo Arrigoni

Senior System Engineer

marrigoni@fortinet.com

Agenda

Overview

2018 Trends Highlights

Q1 Report

FortiGuard Labs Overview

CYBER THREAT ALLIANCE

215
researchers
& analysts

480,000
research hours
per year

8 dedicated labs

Sunnyvale
Vancouver
Ottawa
France
Singapore
Taiwan
Tokyo
Kuala Lumpur

Presence in
31
countries

Research

Development

Innovation

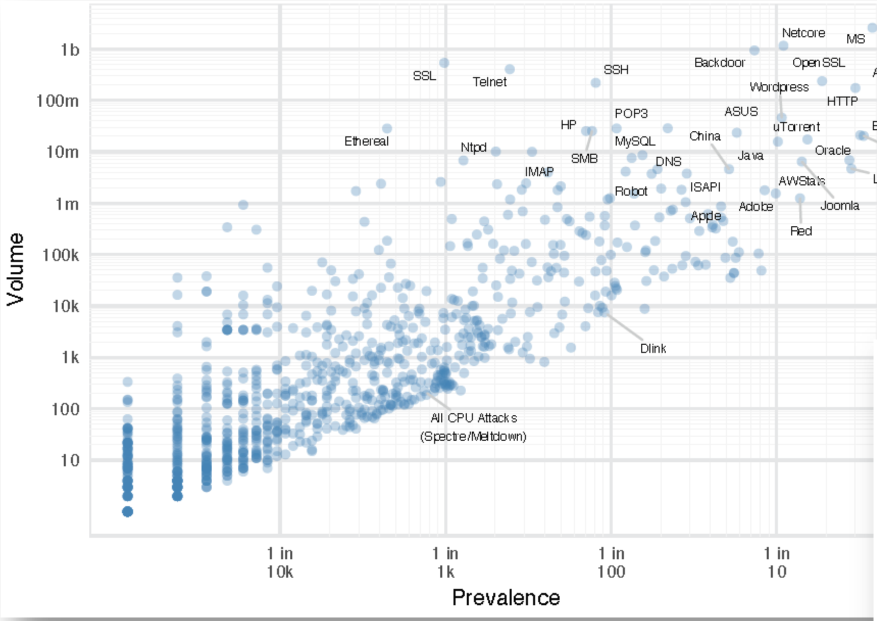
Response

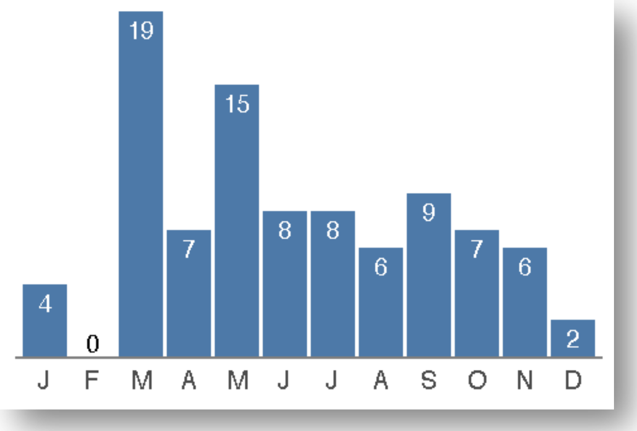
Outreach

Education

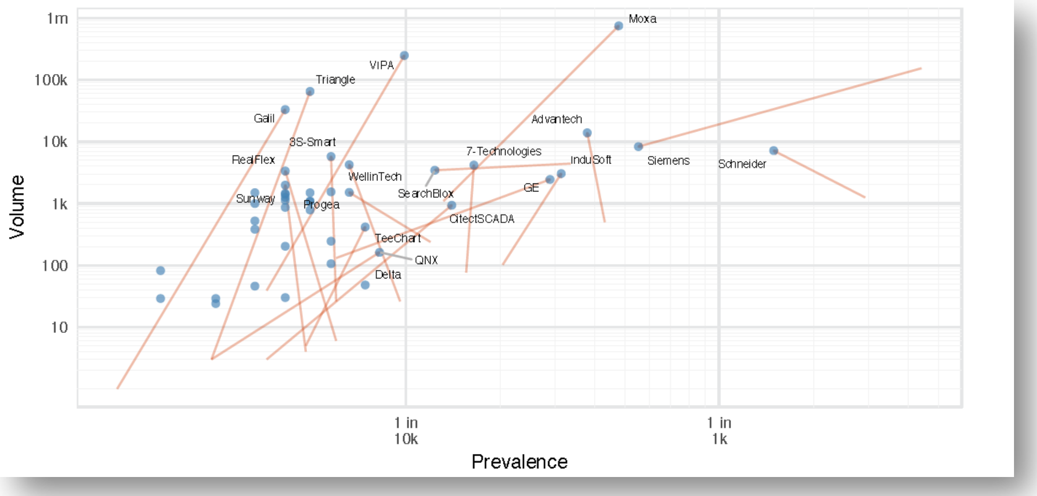
100 Billion
security events a day

Threat Landscape Report 2018





We don't like surprise in this profession



CPU exploits 1 in 3,000 organizations
Attacks targeting Apache 1 in 6 organizations.

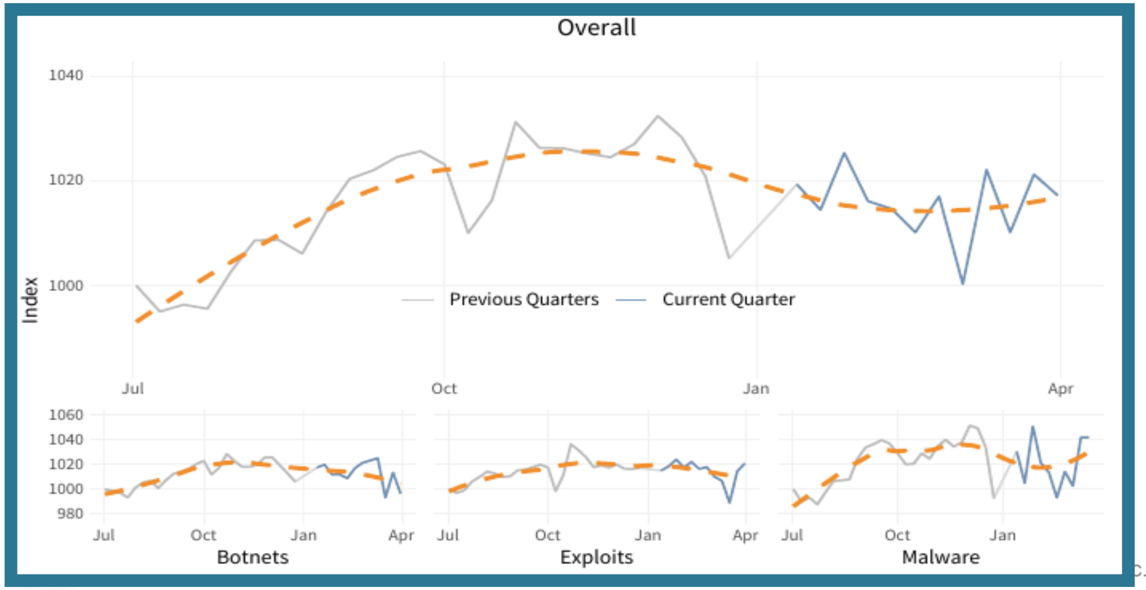
ICS Q4 vs Q1.

Q1 Report

Threat Landscape Index

Is the Threat Landscape Getting Better or Worse?

- Q1 had more volatility than previous quarters – especially for malware
  - 40 malware families, made the weekly top 5 list over the quarter – when measured by volume per device
  - But the shift wasn't extraordinary
- Overall, the threat landscape index rose slightly over 1% in Q1

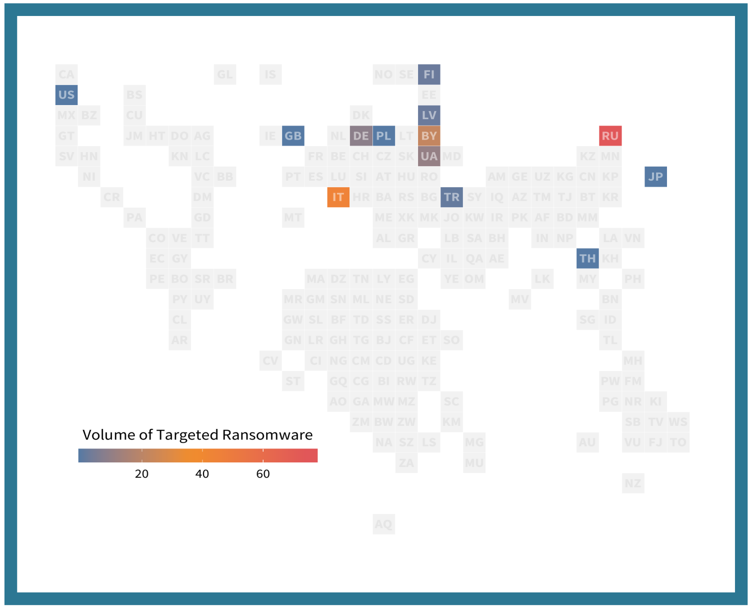


Fortinet Threat Landscape Index (top) and subindices for Botnets, Exploits, and Malware (bottom)

Ransomware: Targeted & Tailored

Recent ransomware attacks exhibit a more designer and destructive nature

- Threat actors moving away from indiscriminate ransomware attacks to more targeted – more lucrative campaigns
- **LockerGoga**: disrupted operations at major **Norwegian aluminum manufacturer** – took weeks to remediate. Also targeted two American chemical companies, and a French engineering firm. Malware execution required administrative rights that would **have necessitated an attacker** to have already **gained some sort of privileged** access to the network, there was very little obfuscation. It's also curious that LockerGoga **appears to lock victims** out of their system.
- **Anatova**: pure 64-bit ransomware. Demands payment in **Dash cryptocurrency**. Avoids encrypting anything that impacts stability of system. The actors behind Anatova appear to have taken a cue from the operators of last year's prolific **GandCrab** in demanding ransom payments in Dash cryptocurrency instead of the usual bitcoins Avoids infecting computers being leveraged for malware analysis.
- Russia, Bulgaria, Italy recorded highest volume


CA GL IS NO SE FI
US BS EE
MX BZ CU DK LV
GT JM HT DO AG IE GB NL DE PL LT BY RU
SV HN KN LC FR BE CH CZ SK UA MD KZ MN
NI VC BB PT ES LU SI AT HU RO AM GE UZ KG CN KP JP
CR DM IT HR BA RS BG TR SY IQ AZ TM TJ BT KR
PA GD MT ME XK MK JO KW IR PK AF BD MM
CO VE TT AL GR LB SA BH IN NP LA VN
EC GY CY IL QA AE TH KH
PE BO SR BR MA DZ TN LY EG YE OM LK MY PH
PY UY MR GM SN ML NE SD MV BN
CL GW SL BF TD SS ER DJ SG ID
AR GN LR GH TG BJ CF ET SO TL
CV CI NG CM CD UG KE MH
ST GQ CG BI RW TZ PW FM
AO GA MW MZ SC PG NR KI
ZM BW ZW KM SB TV WS
NA SZ LS MG AU VU FJ TO
ZA MU
NZ
AQ
Volume of Targeted Ransomware
20
40
60

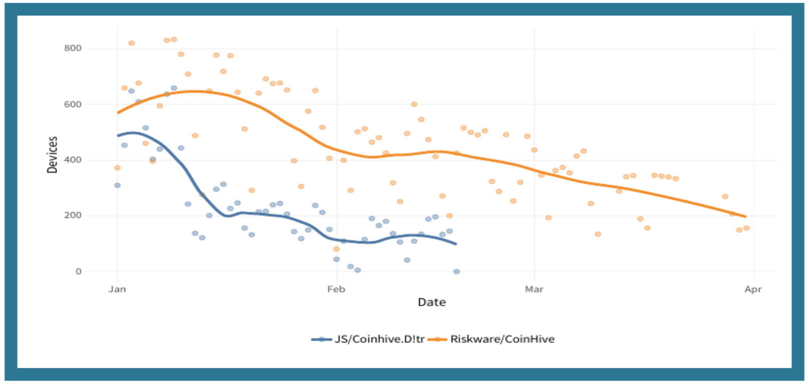
Volume of LockerGoga, Anatova, and GandCrab by country in Q1 2019

This is not typical opportunistic threat geographic distribution. The pattern here suggests targets of choice rather than targets of chance

Cryptocurrency Update

Coinhive – victim of its own success

- Coinhive - the Monero-based cryptomining service shut down in Q1
  - As expected – notable decline in detections of the 2 predominant Coinhive signatures
  - March 8th shutdown is evident for JS/Coinhive variant
  - Riskware/Coinhive signature likely due to lagging remediation of compromised servers
- JavaScript file could be installed on websites to generate income for the site owners
- The Monero transactions between parties were untraceable – which made it attractive to cybercriminals
- Revenue was reported to be $250K a month

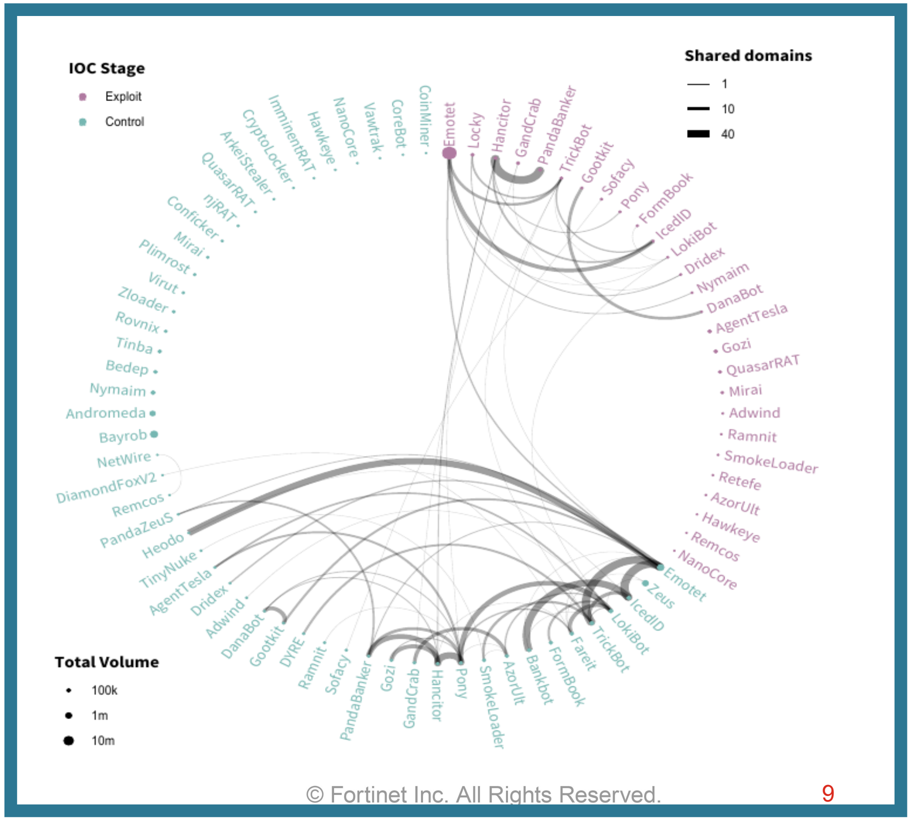


Decline in Coinhive detections during Q1 2019

Shared Infrastructure

Why Buy & Build When You Can Borrow

- Botnets are leveraging established infrastructure
- 60% of threats shared at least one domain
- Rare to find sharing across kill-chain stages
  - Except: 6 key botnets share 9 domains between kill-chain stages

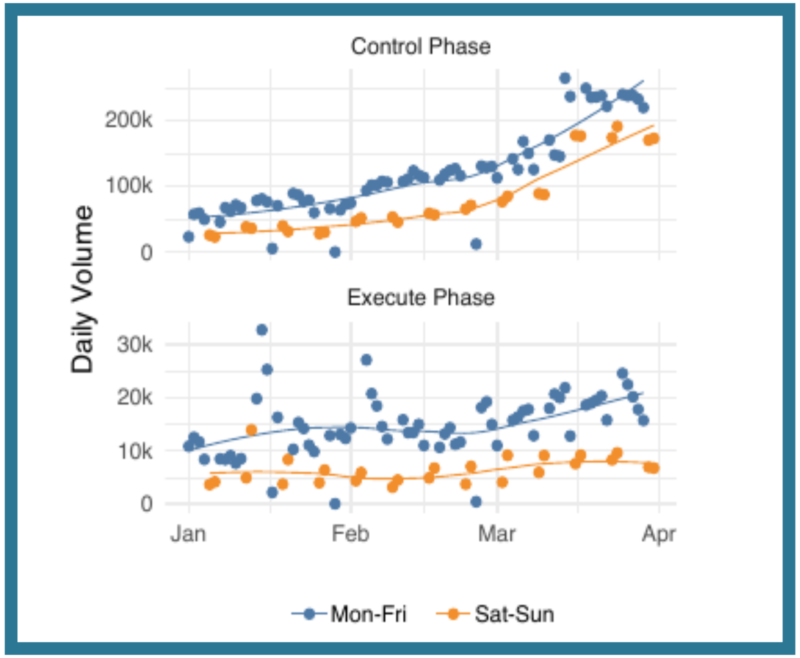


Infrastructure sharing among web filtering detections

Compromised Traffic Timeline

Exploratory Analysis: Web Filtering

- Web traffic blocks and logs attempted access to malicious, hacked or inappropriate websites
- We map type of website and phase of the kill chain where it occurs
- Analysis:
  - Blue dots are weekdays | Orange dots weekends
  - Pre-compromise activity is roughly 3x more likely to occur during workweek
  - Post-compromise traffic shows less differentiation
  - Exploitation requires someone to click on something (phishing email, etc.), while C&C activity does not and can occur at any time



Comparison of web filtering volume for two Cyber Kill Chain phases during weekdays (blue) and weekends (orange).

FORTINET®