



CROWDSTRIKE

CROWDSTRIKE

SANDEEP RAO
SALES ENGINEER, INDIA & SAARC
PH: + 91 99670 94284

LEO THOMAS
ACCOUNT MANAGER, SOUTH
PH: + 91 97314 45784

BREACHES ARE EVERYWHERE



2019 Data Breach Investigations Report

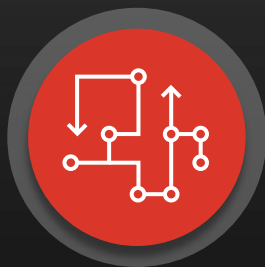
Three key takeaways from the 2019 Verizon Data Breach Investigations Report

1. Understand the attack vendors used by adversaries
 - 60 per cent of breaches involved simple techniques such as phishing and stolen credential, not malware
2. Detection of breaches remains very slow
 - 56% of breaches took months or longer to discover
3. Companies still suffer bad hygiene

KEY CYBERSECURITY CHALLENGES



**ATTACK
SOPHISTICATION**



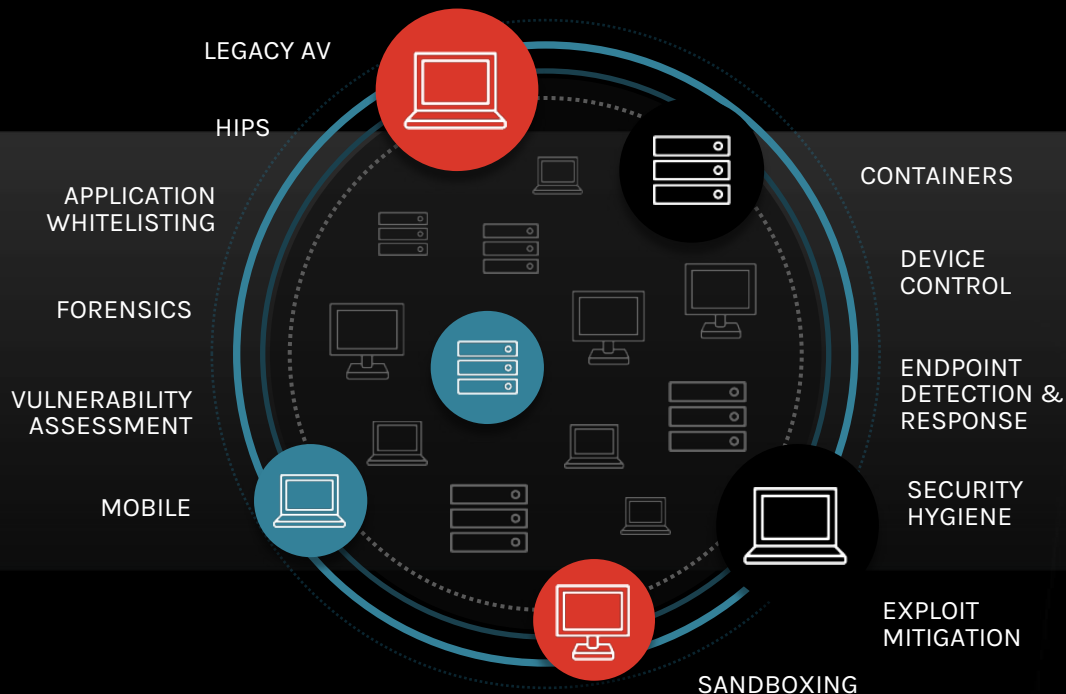
**SOLUTION
COMPLEXITY**



**SKILLS
SHORTAGE**



MULTIPLE AGENTS FOR DIFFERENT NEEDS:



COSTLY TO DEPLOY

DIFFICULT TO MAINTAIN

POOR USER PRODUCTIVITY

REDUCED SECURITY EFFECTIVENESS



CHALLENGES WITH BUILDING A TEAM



STAFF UP

Hire 3-6
skilled FTE



TOOL UP

Acquire necessary
tools for responders



TRAIN UP

Train responders and
keep their skills sharp



RETAIN

Promote and retain
your responders



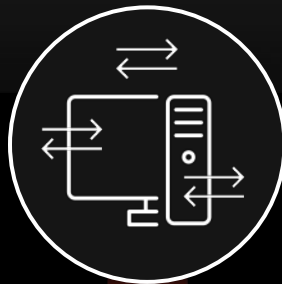
WHAT SHOULD WE ADDRESS TO IMPROVE OUR SECURITY:

**ON-PREM INFLEXIBLE
TO EVOLVING NEEDS**



CLOUD

AGENT BLOAT



**REDUCE MULTIPLE
AGENTS**

**SIGNATURES DON'T WORK
- MISS NEW ATTACK TYPES**



**SIGNATURELESS
SOLUTION**



KNOW YOUR ADVERSARY

AT THE HEART OF EVERY ATTACK IS A HUMAN ADVERSARY.
FALCON INTELLIGENCE REVEALS THEIR MOTIVATION AND TRADECRAFT TO KEEP YOU ONE STEP AHEAD.





MAZE RANSOMWARE



WHAT?

- RANSOMWARE FAMILY USING CHACHA & RSA-2048 TO ENCRYPT MOST FILES ON A VICTIM'S SYSTEM
- SENDS INFORMATION ABOUT VICTIM MACHINE, USERNAME, HOSTNAME, & DISK CAPACITY TO A SET OF IP ADDRESSES
- CAN BE EXECUTED W/OR W/OUT A COMMAND-LINE ARGUMENT
- ABILITY TO ESCALATE PRIVILEGES BY EXPLOITING VULNERABILITIES FROM CVE-2016-7255 AND CVE-2018-8453
- ALTHOUGH PRIMARILY BIG GAME HUNTING FOCUSED, HAS BEEN DISTRIBUTED BY EXPLOIT KITS & SPAM



Maze Ransomware

Dear [REDACTED] your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor

These algorithms are one of the strongest
You can read about them at wikipedia

If you understand importance of situation you can restore all files by following instructions in DECRYPT-FILES.html file

You can decrypt 1 file for free as a proof of work
We know that this computer is a home computer
So we will give you appropriate price for recovering





TWISTED SPIDER - ECRIME



WHAT?

- RESPONSIBLE FOR MAZE RANSOMWARE – FIRST OBSERVED AROUND MAY 2019
- MAZE MAY BE USED AS RANSOMWARE-AS-A-SERVICE BUT MORE LIKELY OPERATED BY A SINGLE GROUP



SO WHAT?

- TWISTED SPIDER ENGAGED IN BIG GAME HUNTING, GENERATING \$7.5M IN THEIR HIGHEST 2019 PAYOUT
- ENGAGES IN EXTORTION FOR PAYMENT – FAILURE TO PAY OFTEN RESULTS IN DATA LEAKAGE



WHAT NEXT?

- THREAT INTELLIGENCE REPORTING
- CAMPAIGN TRACKING
- THREAT ACTOR PROFILING

ORIGIN:

EASTERN EUROPE, RUSSIAN FEDERATION

TARGET NATIONS:

AUSTRIA, CANADA, CHINA, COLOMBIA, CZECH REPUBLIC, FRANCE, GERMANY, ITALY, UNITED KINGDOM, UNITED STATES

TARGET INDUSTRIES:

CONSULTING & PROFESSIONAL SERVICES, GOVERNMENT, MANUFACTURING, STATE & MUNICIPAL GOVERNMENT, TECHNOLOGY


TOOLS:

MAZE




THREAT INTEL ON ACTOR PROFILE PAGE

All Actors



ACTOR

TWISTED SPIDER



ORIGINS
Eastern Europe, Russian Federation

LAST KNOWN ACTIVITY
April 2020

COMMUNITY IDENTIFIERS
N/A

RELATED INDICATORS
[See IOCs](#)

TARGET NATIONS
Austria, Canada, China, Colombia, Czech Republic, France, Germany, Italy, United Kingdom, United States

TARGET INDUSTRIES
Consulting & Professional Services, Government, Manufacturing, State & Municipal Government, Technology

TWISTED SPIDER is the criminal group behind the development and operation of Maze ransomware. While the ransomware was first observed in May 2019, the group gained notoriety in November 2019 with their brazen attitude toward victims and their willingness to speak with security researchers as they began using Big Game Hunting (BGH) tactics to target organizations and businesses. While other actors have threatened to release data in the past if the ransom wasn't paid, TWISTED SPIDER has made this act their anthem and created a dedicated website to leak data if victims are unresponsive to the group or refuse to pay ransoms.

Maze ransomware has been observed distributed via exploit kits (EK), spam campaigns, and through acquiring RDP credentials for access. The group is capable of moving laterally and exfiltrating data for extortion. It is likely that TWISTED SPIDER is opportunistic, with targets primarily observed in North America and Europe as well as a few incidents in China and South America. As of February 2020,

Kill Chain

Services Used

- Phishing services
- Exploit Kits, including Fallout EK
- Likely purchase of RDP credentials

Services Offered

Customers

Victims

TWISTED SPIDER targets opportunistically. While observed infections appear to be concentrated in North America and Europe, it is likely the actors target regardless of country, with the exception of countries in the Commonwealth of Independent States (CIS). In regards to sector, there is currently no discernible trend in what sectors are targeted, which further indicates the actor is purely opportunistic in nature.

Crimes

- Accessing a computer without authorization for the purpose of commercial advantage and private financial gain
- Damaging a computer through the transmission of code and commands
- Conspiring to commit fraud and related activity in connection with computers

THE ADVERSARY ARE SWIFT AND FAST

BEAR 00:18:49

GHOLLIMA 02:20:14

PANDA 04:00:26

KITTEN 05:09:04

SPIDER 09:42:23



The background consists of a vibrant red color with a radial pattern of fine, white-to-red gradient lines that converge towards the center, creating a sense of motion and speed. A solid black horizontal band is positioned in the middle of the image, serving as a background for the text.

SPEED IS EVERYTHING:
THE 1-10-60 RULE

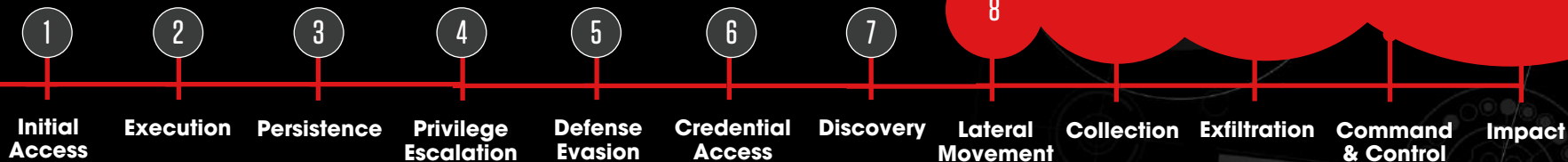
SURVIVAL OF THE FASTEST

**TO STAY AHEAD
YOU MUST:**

**DETECT IN
1min**

**INVESTIGATE IN
10min**

**RESPOND IN
60min**



MITRE ATT&CK PHASE



GARTNER , FEBRUARY 2019

PREPARE FOR ENDPOINT PROTECTION SHIFTING TO THE CLOUD

Recommendations

1. Evaluate cloud-delivered solutions well before your next renewal.
 2. Choose vendors that offer a true elastic and agile cloud architecture supported by a range of service options such as incident response help and managed detection and response.
 3. Seek fully integrated EPP solutions with EDR capabilities that use the same detection funnel, data repository, management console and agent.
 4. Ensure that EPP detection capabilities include more modern behavioural approaches that are immediately adaptive to detect or block new attack techniques.
-

FALCON PLATFORM PROTECTS ALL WORKLOADS



CROWDSTRIKE THREAT GRAPH

WINDOWS LINUX MAC ANDROID IOS

WORKSTATIONS

SERVERS

DATACENTERS

MOBILE
FALCON FOR MOBILE

CLOUD / CONTAINERS
FALCON FOR AWS

IOT

LIGHTWEIGHT AGENT



CROWDSTRIKE STORE APPLICATIONS

A UNIQUE CYBER SECURITY ECOSYSTEM



ADVANCED THREAT HUNTING / DECEPTION



APPLICATION WHITELISTING



ICS / IOT THREAT DETECTION



VULNERABILITY RISK MANAGEMENT



APPLICATION ANALYTICS



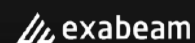
PATCH MANAGEMENT



ATTACK SURFACE MANAGEMENT



UEBA / INSIDER THREAT



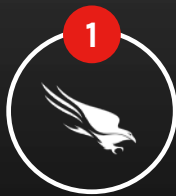
3 SMALL STEPS TO REPLACE YOUR AV



No infrastructure
setup



No fine-tuning,
rule writing



Install the
Falcon Agent



Verify the
installation



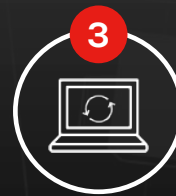
No reboot



No signatures
updates



No scan



Remove legacy
products

Financial Institution

77,000 AGENTS
1 DAY

Hospitality Chain

40,000 AGENT
5 DAYS

Technology Company

55,000 AGENTS
5 DAYS

Financial Institution

300,000 AGENTS
90 DAYS



WHAT WERE THE ANALYST SAYING IN 2018

AND NOW

2017

2018

2019

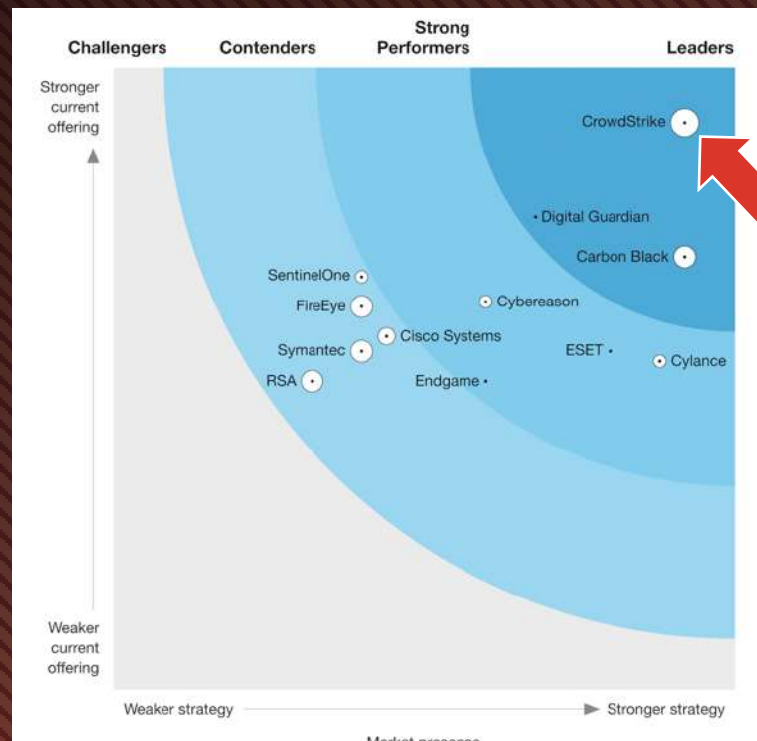


FROM VISIONARY TO LEADER & COMPLETENESS OF VISION IN 3 YEARS

FORRESTER WAVES



Forrester Wave for Endpoint Security Suites, Q2 2018



Forrester Wave for Endpoint Detection and Response, Q3 2018



THE NEW STANDARD IN ENDPOINT PROTECTION

INDUSTRY ANALYSTS

Gartner

“CROWDSTRIKE NAMED A LEADER IN THE 2019 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION AND POSITIONED FURTHEST FOR COMPLETENESS OF VISION”

FORRESTER®

“CROWDSTRIKE IS THE ONLY VENDOR TO BE NAMED A LEADER IN BOTH ENDPOINT SECURITY SUITE AND EDR WAVES”

IDC

“LEADER IN IDC MARKETSCOPE FOR US INCIDENT READINESS, RESPONSE AND RESILIENCY SERVICES”

PRODUCT REVIEWS AND TESTS

AV comparatives

“FALCON CERTIFIED TO REPLACE LEGACY ANTIVIRUS”

SE Labs

“FALCON ACHIEVES AAA RATING IN SE LABS TEST”

MITRE

“MITRE VALIDATES FALCON AGAINST ATT&CK™ FRAMEWORK”

SC

“FIVE STAR RATING AND BEST BUY AWARD”

Gartner peerinsights



CUSTOMER INSIGHTS

HIGHEST SCORE OF 4.9/5 IN BOTH EDR AND ENDPOINT PROTECTION PLATFORMS

AWARDS AND RECOGNITION

Winner SC Awards

NAMED BEST SECURITY COMPANY FOR TWO CONSECUTIVE YEARS

CNBC DISRUPTOR 50 2017

CROWDSTRIKE NAMED CNBC DISRUPTOR FOR TWO CONSECUTIVE YEARS

Forbes

FORBES CLOUD 100 LIST FOR TWO CONSECUTIVE YEARS

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. Gartner Peer Insights 'Voice of the Customer': Endpoint Detection and Response Solutions, 28 February 2019 and Gartner Peer Insights 'Voice of the Customer': Endpoint Protection Platforms, 19 December 2018. <https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms> and <https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions>



FORRESTER TOTAL ECONOMIC IMPACT (TEI) STUDY

OF CROWDSTRIKE FALCON®



In October 2019
Forrester Research
was commissioned
to conduct an ROI
study of the
CrowdStrike
Falcon Platform



ROI
316%



PAYBACK
< 3 MONTHS



The Top 25 Cybersecurity Companies of 2019

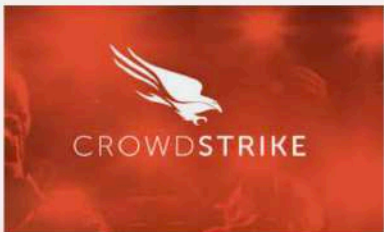
December 10, 2019



The Software Report is pleased to announce The Top 25 Cybersecurity Companies of 2019. For the past two months, we collected hundreds of nominations from professionals in the cybersecurity field. They provided their candid feedback on the strength of each company's technology, caliber of the company's organization, management team effectiveness and ability to stay ahead of the latest

cybersecurity threats, among other attributes.

After thorough review of each company's nomination survey results, we selected those who scored the highest. We paid particular attention to those who demonstrated consistency across each performance area. The following company awardees represent this year's best of the best in cybersecurity.



1. CrowdStrike

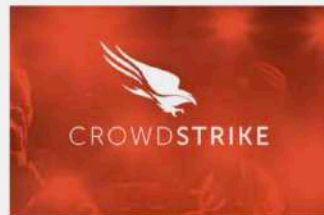
Category: Endpoint Security

Location: Sunnyvale, California

Founded in 2011, CrowdStrike was borne out of the realization that existing security solutions on the market weren't enough to combat the sophisticated hackers that were infiltrating some of the nation's



<https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2019/#.XfKfWIRoHrE.linkedin>



1. CrowdStrike

Category: Endpoint Security

Location: Sunnyvale, California

Founded in 2011, CrowdStrike was borne out of the realization that existing security solutions on the market weren't enough to combat the sophisticated hackers that were infiltrating some of the nation's

largest and well-known corporations. Co-founders George Kurtz and Dmitri Alperovitch made a bet that marrying advanced endpoint protection with intelligence would be a better way to identify the perpetrators behind the attacks. And that bet has paid off. Today CrowdStrike is a premier cyber security company with presence in the U.S., Europe, and India. It employs about 2,000 and counts ADP, Rackspace, and Hyatt among its clients. The company provides security services to 12 of the 20 Fortune largest global companies, ten of the 20 largest financial institutions and five of the top ten largest healthcare providers. It's also a leading cybersecurity provider for the energy market.

CrowdStrike CEO Kurtz, a serial entrepreneur, is an internationally recognized cybersecurity expert, holding executive roles at McAfee before creating CrowdStrike with Alperovitch. His company was also who the Democratic National Committee turned to when it suspected it was hacked during the run-up to the 2016 election. CrowdStrike's IPO occurred in June of 2019.



CUSTOMER TRUSTED



44 OF 100

FORTUNE 100 COMPANIES



37 OF 100

TOP GLOBAL COMPANIES



9 OF 20

MAJOR BANKS



5 OF THE TOP 10

LARGEST HEALTHCARE PROVIDERS



7 OF THE TOP 10

LARGEST ENERGY INSTITUTIONS



BERIN LAUTENBACH
CISO APAC,
Telstra



JOHN VISNESKI
Director, Information
Security & Data Prot.,
Pokémon Company
International



ROBERT THOMAS
Chief Operating Officer,
Mercedes-AMG
Petronas Motorsport



ROLAND CLOUTIER
Sr. VP,
Chief Security Officer,
ADP



NIK PATEL
Head of Technology
Security Services,
Credit Suisse



SCOTT STOOPS
Security Analyst,
Ashland University





START YOUR FREE TRIAL

crowdstrike.com/freetrial

