CROWDSTRIKE

2019 GLOBAL THREAT EXECUTIVE SUMMARY:
ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED

ELIA ZAITSEV, VP SALES ENGINEERING & ARCHITECTURE - AMERICAS

A LITTLE **ABOUT ME:**

Elia Zaitsev

- First SE at CrowdStrike
- Over a decade of industry and beard growing experience
- Extensive experience in adversary tradecraft, especially “living off the land” techniques

AGENDA

1. Threat Landscape by the numbers
2. Understanding Today's Adversaries
3. Recommendations

CROWDSTRIKE

WHERE IS THIS INFO COMING FROM?

CROWDSTRIKE

CROWDSTRIKE'S ECOSYSTEM

ENDPOINT PROTECTION

THREAT INTELLIGENCE

IR & STRATEGIC ADVISORY SERVICES

MANAGED HUNTING & Remediation

THREAT LANDSCAPE BY THE NUMBERS

LEVERAGING THE POWER OF THREAT GRAPH TO UNCOVER COMPELLING STATISTICAL INSIGHTS FROM 2018

CROWDSTRIKE

THREAT GRAPH INSIGHTS

Understanding Attack Types, Targets and Trends Using the Threat Graph

THREAT GRAPH CAPABILITIES

320 Billion
Events per day

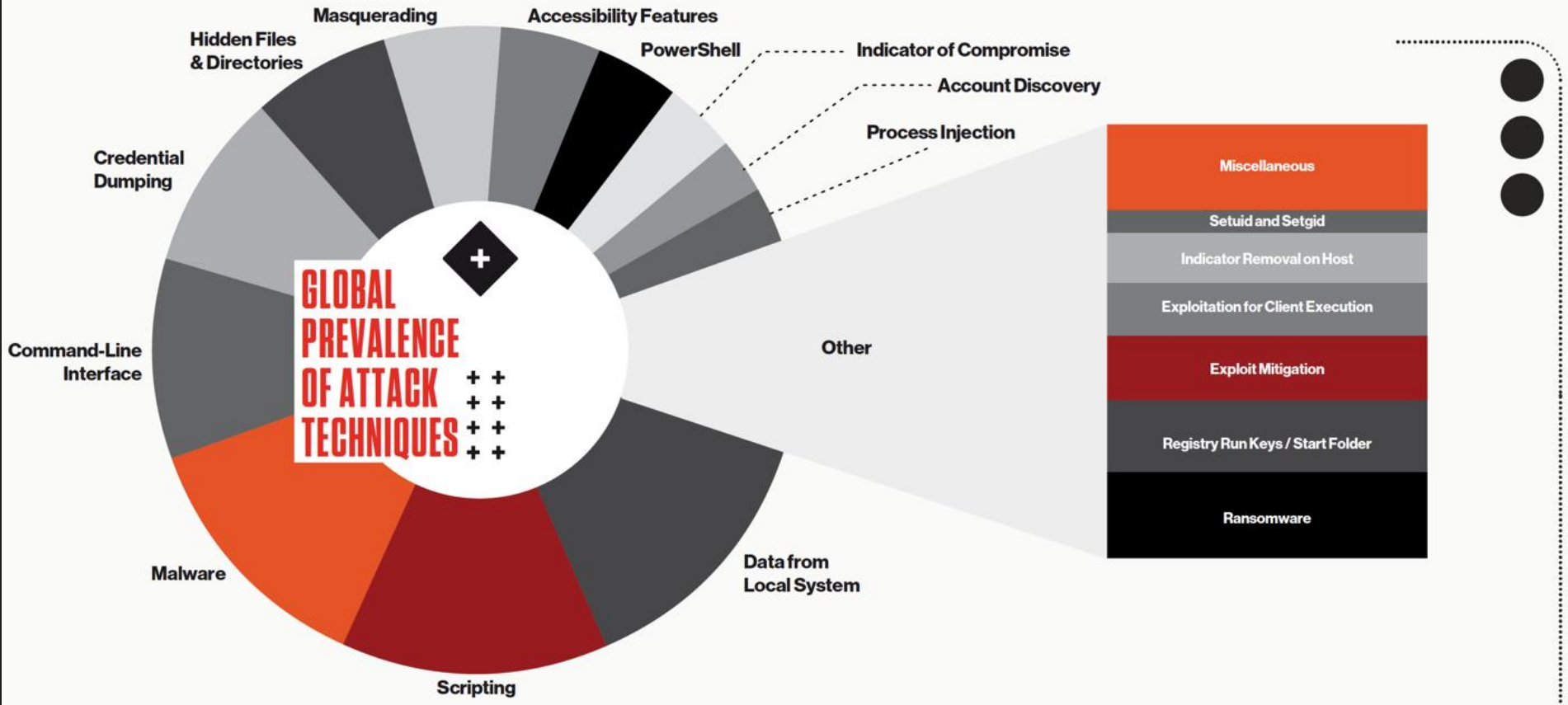
4 Million
Peak events per second

>3 Million
Average events per second

- CrowdStrike Threat Graph is the brains behind the CrowdStrike Falcon platform.
- Falcon agents are deployed in more than 176 different countries and capture more than 1 trillion events every week.

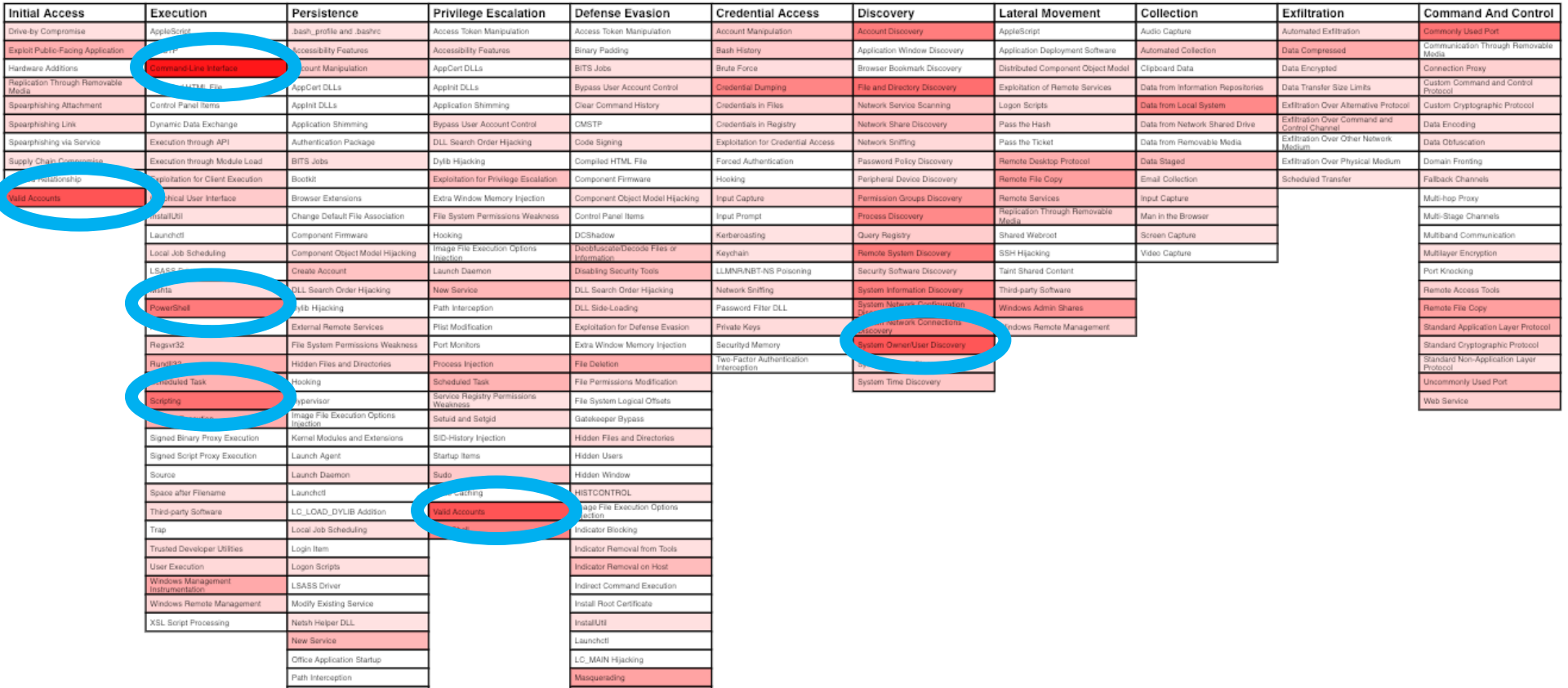
CROWDSTRIKE

GLOBAL PREVALENCE OF ATTACK TECHNIQUES



CROWDSTRIKE

MITRE ATT&CK HEAT MAP



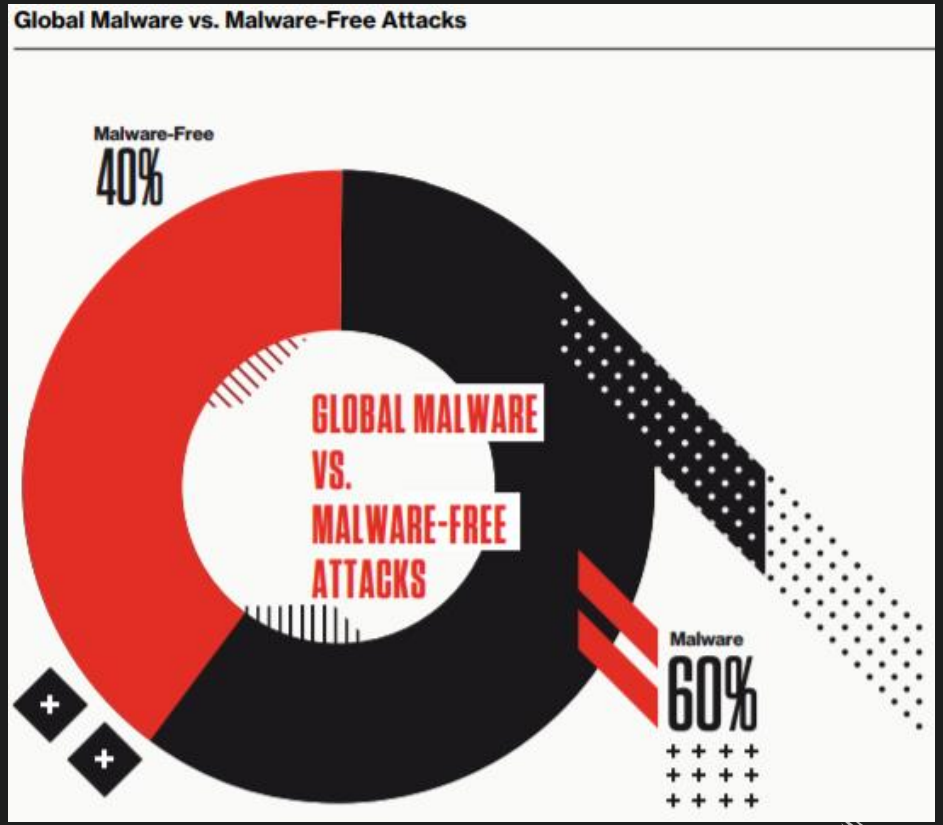
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	[illegible]	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	[illegible]count Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	[illegible] HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
[illegible]Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	[illegible]chical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS [illegible]	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	[illegible]shta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	[illegible]ylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration [illegible]	Windows Admin Shares			Remote File Copy
	[illegible]	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	[illegible] Network Connections Discovery	[illegible]ndows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	[illegible]				Standard Non-Application Layer Protocol
	[illegible]cheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	[illegible]ypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	[illegible]	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	[illegible] Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	[illegible]age File Execution Options Injection						
	Trap	Local Job Scheduling	[illegible]	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		Launchctl						
		Office Application Startup		LC_MAIN Hijacking						
		Path Interception		Masquerading						

MITRE ATT&CK HEAT MAP

Initial Access	Execution	Privilege Escalation	Discovery
Valid Accounts	Command line interface	Valid Accounts	System Owner/User Discovery
	PowerShell		
	Scripting		

BEYOND MALWARE

- Malware attacks: Simple use cases where a malicious file is written to disk and Falcon detects and/or prevents the attempt to run that file
- Malware-free attacks: Those in which the initial tactic did not result in a file or file fragment being written to disk. Examples of this include attacks where code executes from memory or where stolen credentials are leveraged for remote logins using known tools.

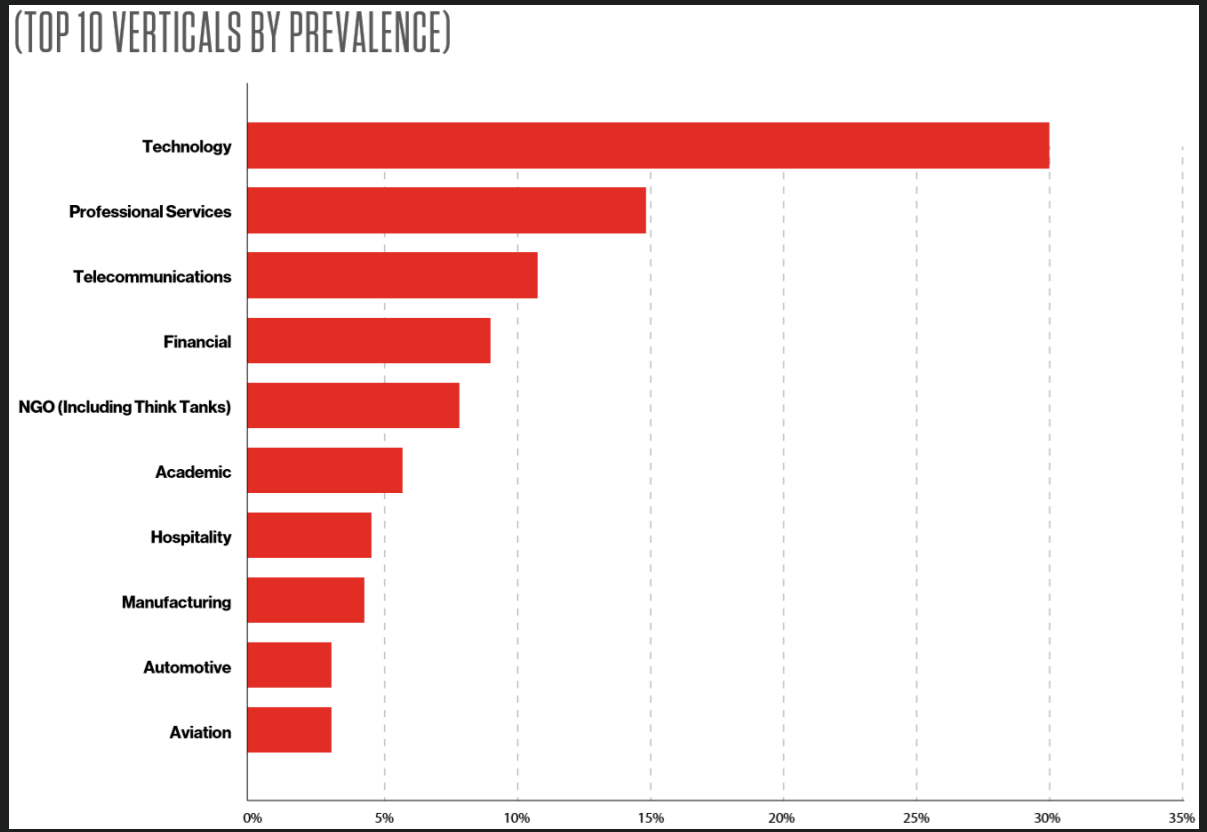


CROWDSTRIKE

MALWARE VS MALWARE-FREE BY INDUSTRY

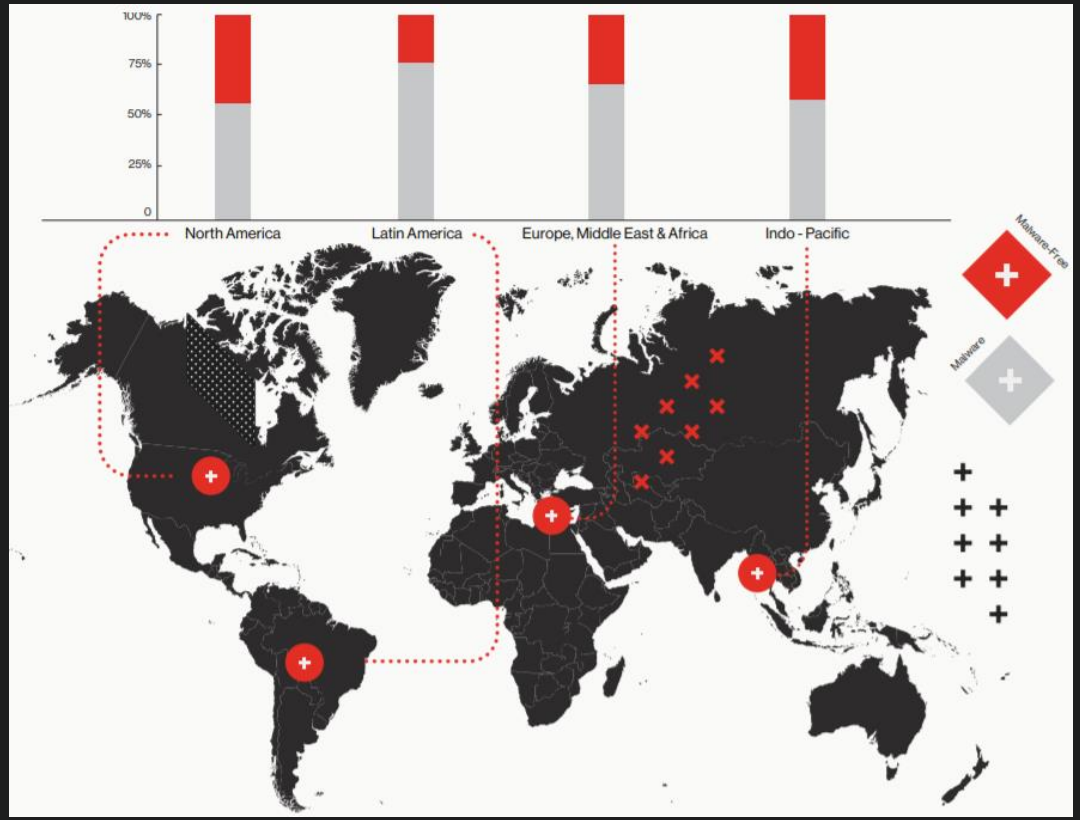
CROWDSTRIKE

ALL CAMPAIGNS BY INDUSTRY



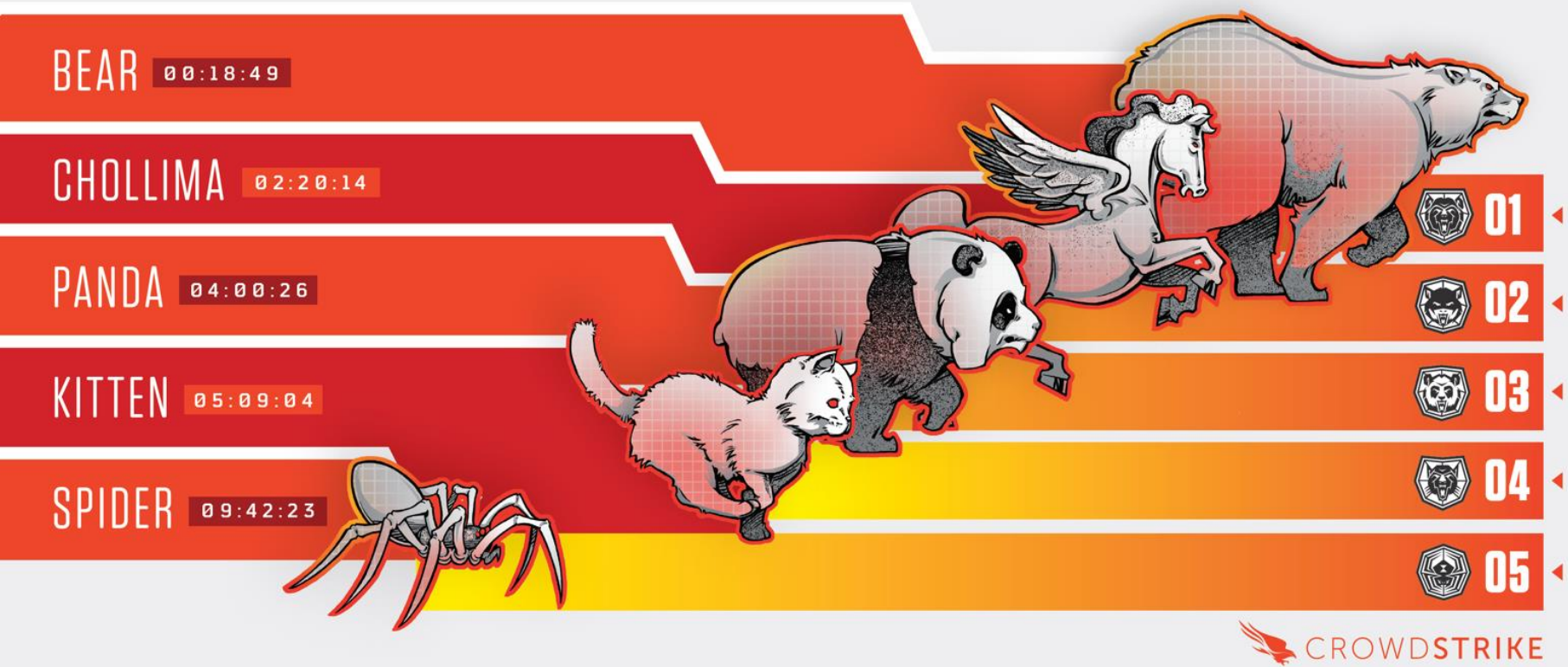
CROWDSTRIKE

MALWARE VS MALWARE-FREE BY REGION



CROWDSTRIKE

BREAKOUT TIME BY REGION



CROWDSTRIKE

UNDERSTANDING TODAY'S ADVERSARIES

THREAT ACTOR MOTIVATIONS

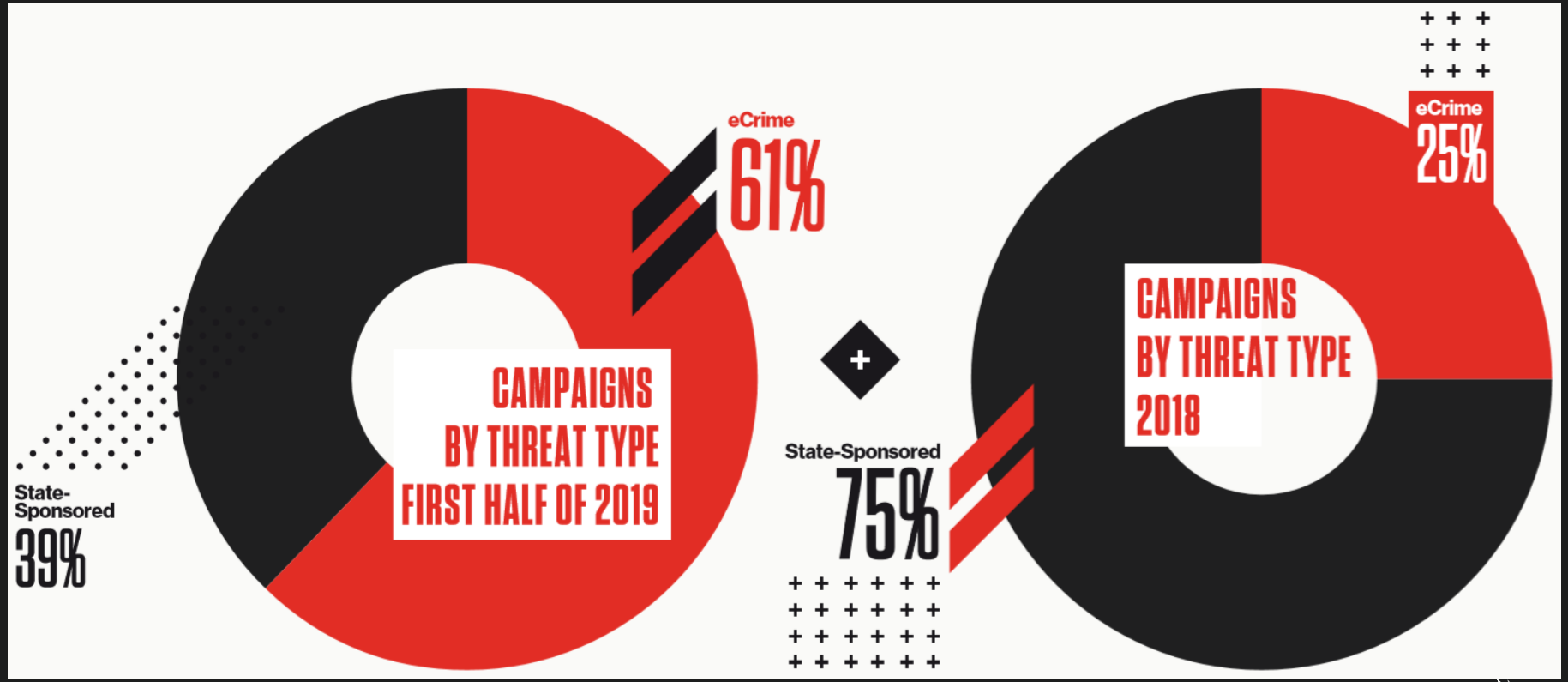
Nation State/Targeted Attackers

eCrime

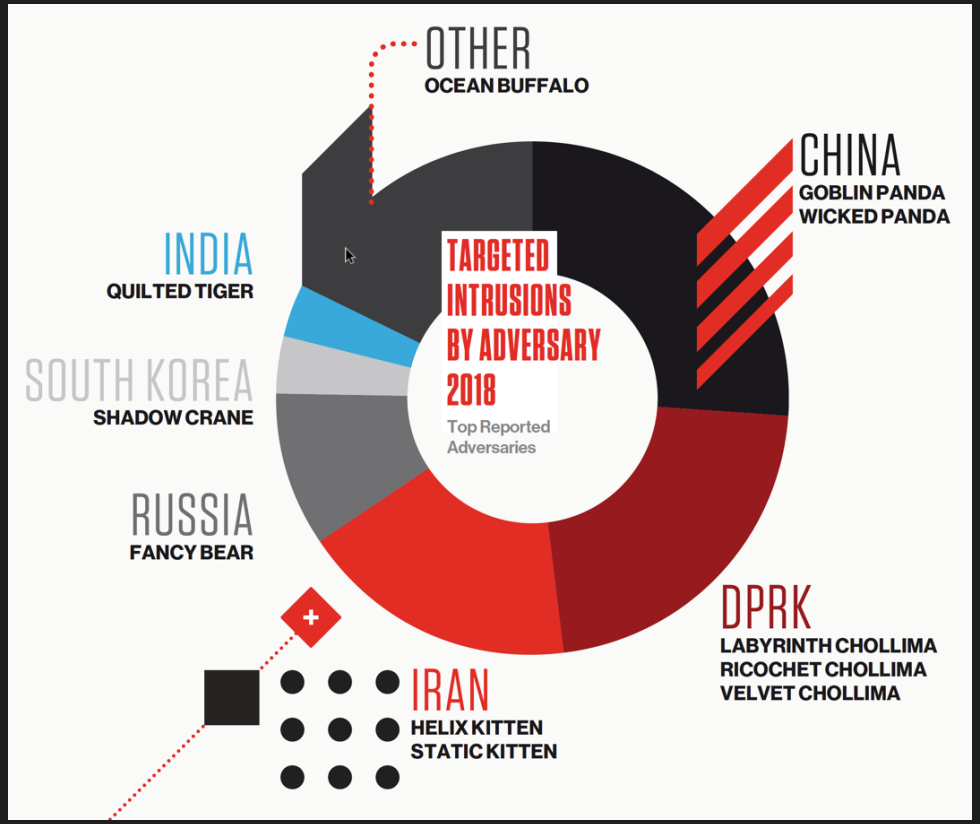
Hacktivist

CROWDSTRIKE

State Sponsored vs eCrime Campaign Prevelance



2018 Targeted State-Sponsored Intrusions by Region



CROWDSTRIKE

OVERWATCH INTRUSION REPORT

Unidentified State-Sponsored Adversaries: Targeting Linux Networks at Telecom Providers

Compromised Linux Host

Defense Evasion

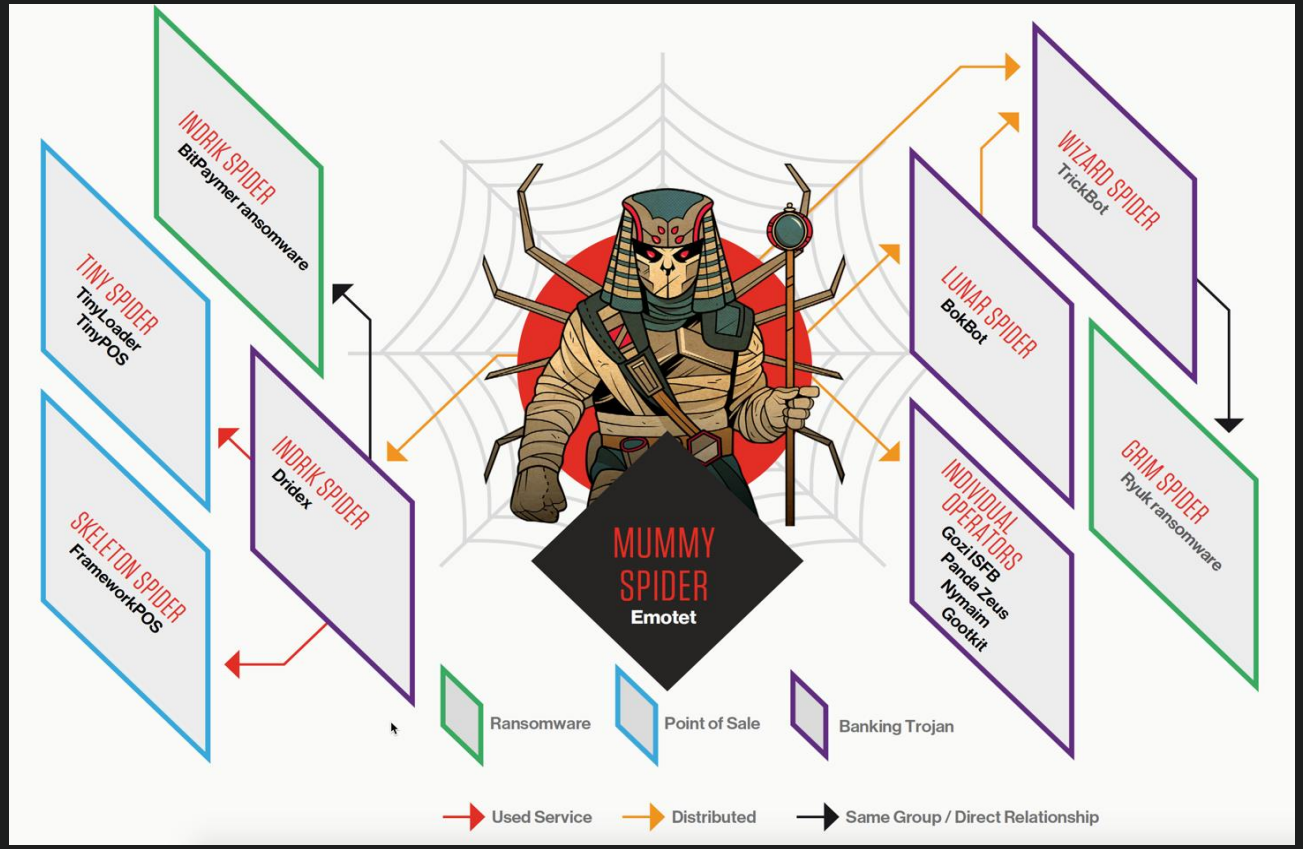
- Compromised Linux host used as beachhead, staging host
- Used base64-encoded Perl commands and GNU tar for staging exfil of config files and bash history files
- Extensive efforts to cover tracks
- Backdoored SSHd to allow return access
  - This “version” was globally unique in our data set

CROWDSTRIKE

MUMMY SPIDER

Malware Delivery Service

- Support for multiple established eCrime adversaries
- Geo-targeting focused on victims in U.S., UK, and Canada; expanded to include Germany late in 2018



CROWDSTRIKE

OVERWATCH INTRUSION REPORT

MUMMY SPIDER: Unprecedented Volume in Massive Emotet Campaign

“Big Game Hunting”

Phishing Campaign Targeting Enterprise

- Significant phishing campaign affected more than 270 CrowdStrike customers in November 2018
- Macro-enabled MS Word Doc sent as email attachment
- If Doc ran /w Macros enabled obfuscated PowerShell command would call C2 and retrieve first-stage implant
- Additional 2nd-stage malware retrieved and installed, based on geolocation of infected host
- Blocked By Falcon Endpoint

CROWDSTRIKE

EMOTET IS ALIVE AND WELL

Non-Targeted eCrime Malware (in order of prevalence)

01	02	03	04	05
EMOTET	TRICKBOT	CRYPTOCURRENCY MINERS (VARIOUS)	GOZI/URSNIF/RM3	DRIDEX

CROWDSTRIKE

OVERWATCH INTRUSION REPORT

STARDUST CHOLLIMA: One of the Many Threats Facing the Financial Industry

Use of Valid Credentials

Extensive Use of "Living off the Land" Techniques

- Threat actor used established beachhead within network to move laterally
- Scheduled tasks and WMI created PowerShell reverse-shells and RDP tunnels
- Valid creds belonged to network admins
- Domain Controllers were one of first hosts accessed from beachhead
- Used LDIFDE utility to export AD data, accessed LSASS in attempt to dump more creds

CROWDSTRIKE

OVERWATCH INTRUSION REPORT

STARDUST CHOLLIMA: One of the Many Threats Facing the Financial Industry

Use of Valid Credentials

Extensive Use of "Living off the Land" Techniques

- Accessed payment processing server
- PowerShell used to access documents containing sensitive financial information
- Unique tool, log.exe used for executing malicious DLL payload network tunneling; injected payloads into legitimate Explorer.exe memory space
- After customer stopped breach with OW assistance, IR team discovered initial vector was publicly exposed unsecured network monitoring system without endpoint software

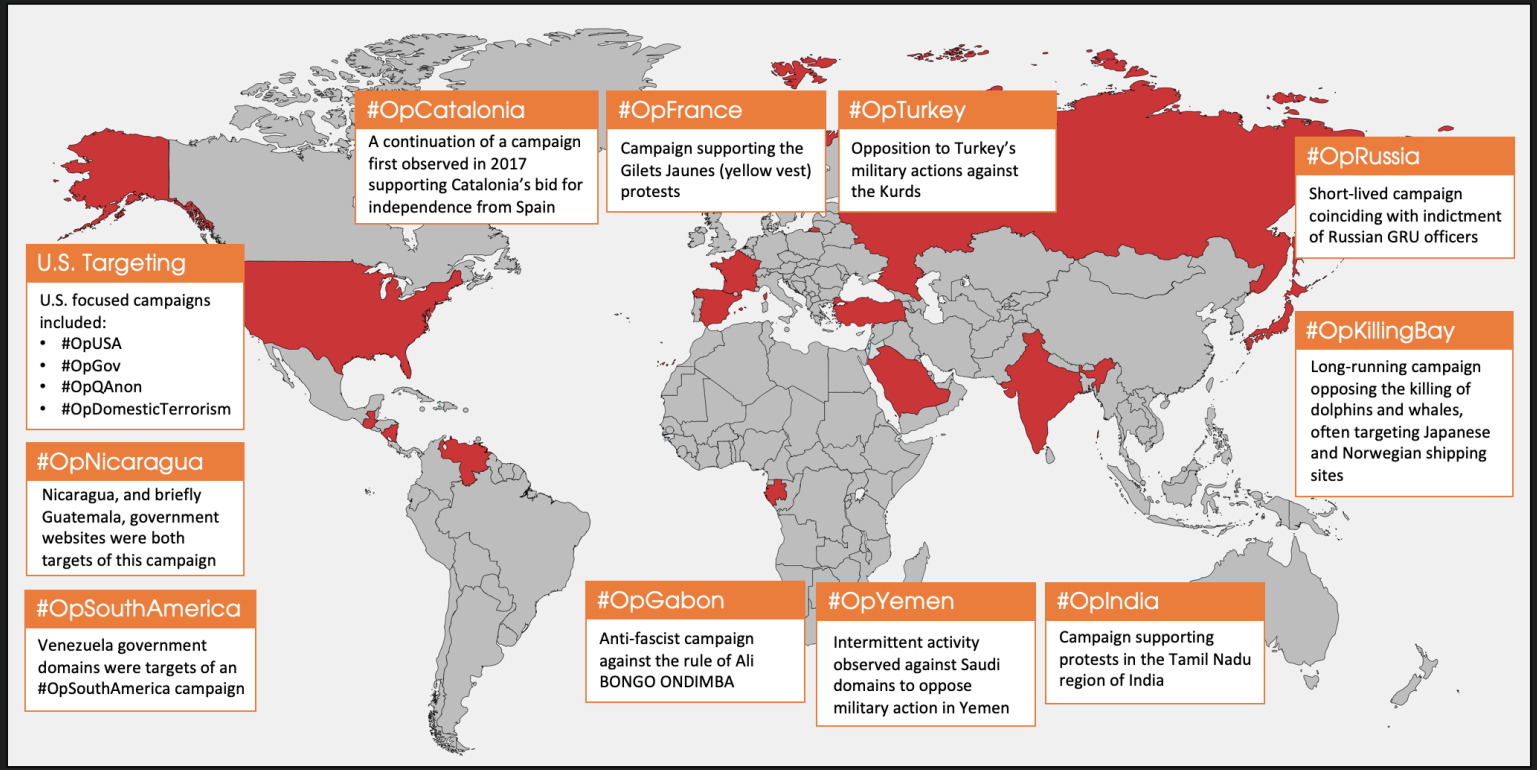
CROWDSTRIKE

CROWDSTRIKE SERVICES CASE STUDY

An Employee Satisfaction Survey Was a Front for a Payroll Heist

- Spearphish Email
- Executive Hook
- False Survey Page
- Browser Vulnerability
- Obtained and Used Intelligence
- Interception
- Money

Anonymous Operations



RECOMMENDATIONS

RECOMMENDATIONS:

BASIC SECURITY HYGIENE STILL MATTERS

- User Awareness combats phishing and related social engineering techniques
- Asset management and software inventory
- Vulnerability and patch management
- Multi-factor Authentication and Privilege Management
- Password protection for endpoint security software

RECOMMENDATIONS

LOOK BEYOND MALWARE: STRENGTHEN DEFENSES AGAINST MODERN ATTACK

- Unusual use of native tools
- PowerShell
- Windows and non-Windows
- Alternate methods of code execution, persistence, stealth, command and control

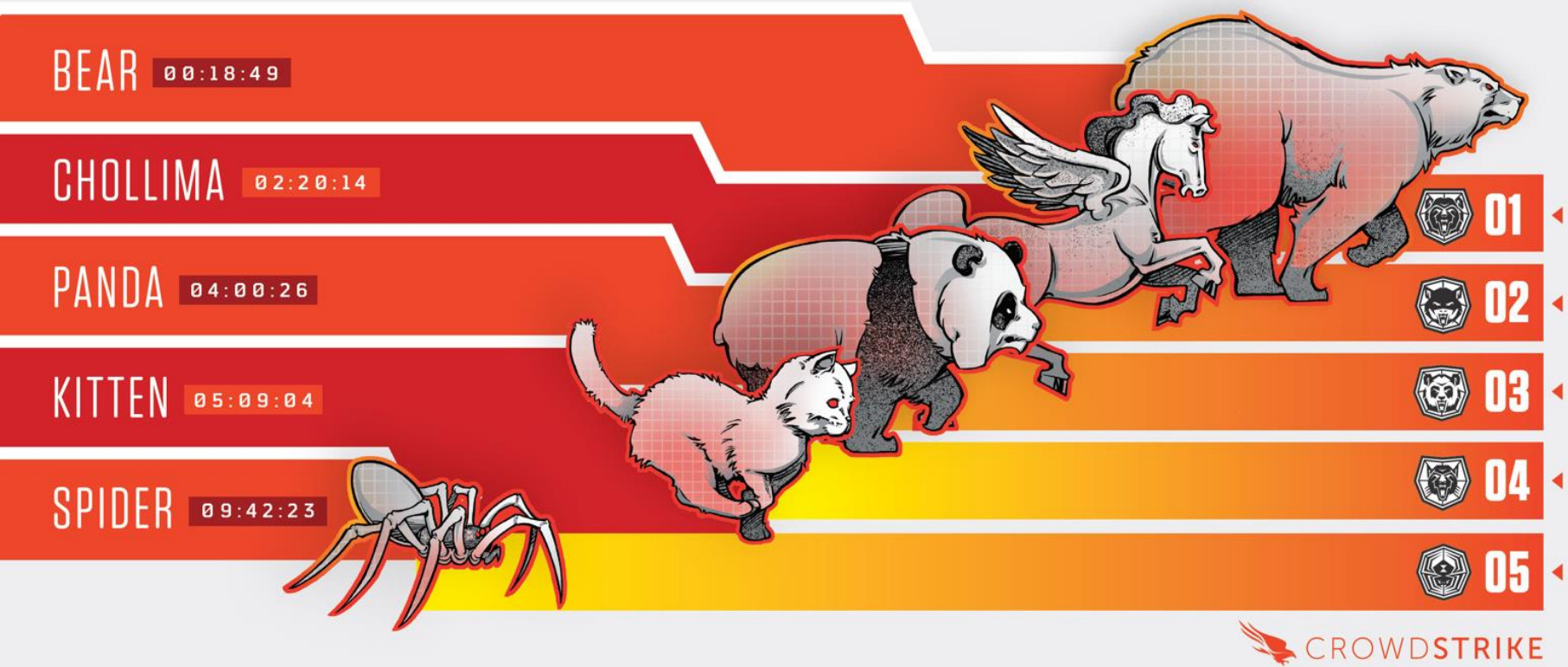
RECOMMENDATIONS

LOOK TO PARTNERS TO HELP SOLVE THE SKILLS SHORTAGE

- Behind every attack, there is a human adversary
- They are adept at changing TTPs in response to technical controls – technology alone won't protect you
- Defense requires effective, dedicated, capable security professionals – but they can be expensive and hard to find/keep
- Partnering with best-in-class external solution providers to help fill skills shortages in a cost-effective manner

CROWDSTRIKE

BREAKOUT TIME BY REGION



CROWDSTRIKE


SPEED IS EVERYTHING:
THE 1-10-60 RULE

CROWDSTRIKE

SURVIVAL OF THE FASTEST:
THE 1 - 10 - 60 RULE

TIME TO DETECT

1 MIN

TIME TO INVESTIGATE

10 MIN

TIME TO REMEDIATE & CONTAIN

60 MIN

THANK YOU!

The full 2019 Global Threat Report is available for free at:

https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

The Overwatch 2019 Mid-Year Report is available for free at:

https://www.crowdstrike.com/resources/reports/observations-from-the-front-lines-of-threat-hunting-2019/