Detecção Agnóstica de Ransomware

NICHOLS JASPER

37º GTS

24/10/2022

Agenda

Introdução
- Conceitos
- Impactos Diretos e Indiretos
- Panorama de Ransomware
- Quem é o meu Adversário?
- Vetores de Ataque
- Atores de Ameaça / Grupos de Ransomware

Detecção
- MITRE TID
- IOCs e IOAs
- Espectro Detectivo
- Ransomware Kill Chain
- Priorização de TTPs
- Conclusão
- Q&A

Whoami

Formado em Processamento de Dados na FATEC-SP e pós-graduado em Gestão de Segurança da Informação pelo IBMEC.

Professor da disciplina de SI no curso de ADS na FATEC-SP há 11 anos.

14 anos de experiência na área de SI, 6 focados em segurança cibernética. Atualmente na posição de especialista em detecção de ameaças da Santander Global Tech.

CISSP, SANS GCDA e GDAT, CCSK em andamento.

Presente por aqui desde o GTS 12 (2008).

DISCLAIMER – Tudo o que for dito daqui em diante reflete minhas opiniões pessoais e não necessariamente a visão do meu empregador.

Introdução - Conceitos

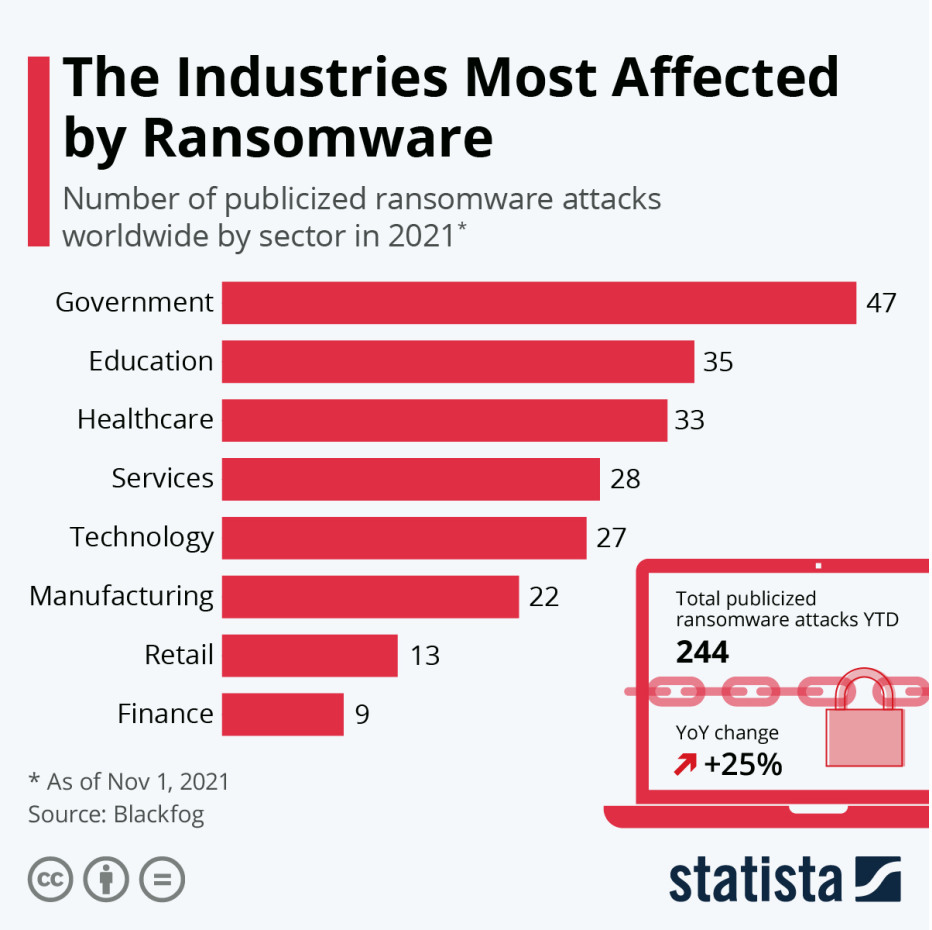
De acordo com a Mandiant [1] Ransomware pode ser definido como *"Um programa cujo propósito principal é realizar alguma ação maliciosa (como criptografar dados), com o objetivo de extrair pagamento da vítima para evitar ou desfazer uma ação maliciosa previa."*

Além do impacto operacional direto, há diversos outros custos, como por exemplo [2]:

> Tempo de inatividade e perda de negócios.
> Danos à reputação da marca.
> Esforços de recuperação de dados.
> Despesas legais relacionadas a regulamentação e conformidade e sanções.
> Práticas de segurança pós-infecção.

Panorama de Ransomware - Dados Gerais

- 127 novas famílias de ransomware foram descobertas em 2020, um aumento de 34% em relação a 2019
- 90% das instituições financeiras foram alvo de ataques de Ransomware.
- O custo médio de um incidente de ransomware foi de $4.62 milhões em 2021, sem incluir o resgate.
- O custo global relacionado a ransomware está previsto para alcançar 20 bilhões de dólares em 2021.



[3] Panda Security, Varonis, IBM, Cybersecurity Ventures and Statista

Panorama de Ransomware – Inovações de 2021

- Técnicas de multi-extorsão [4] para "encorajar" a vítima a pagar mais rapidamente.
- Ataques a cadeia de suprimentos, atacando computadores da organização e de seus fornecedores.
- Sites com *leaks* na Dark Web para expor as vítimas, muitas vezes expondo também seus clientes.
- Ameaça de ataques DDoS adicionais para forçar o pagamento e indisponibilizar canais de comunicação.

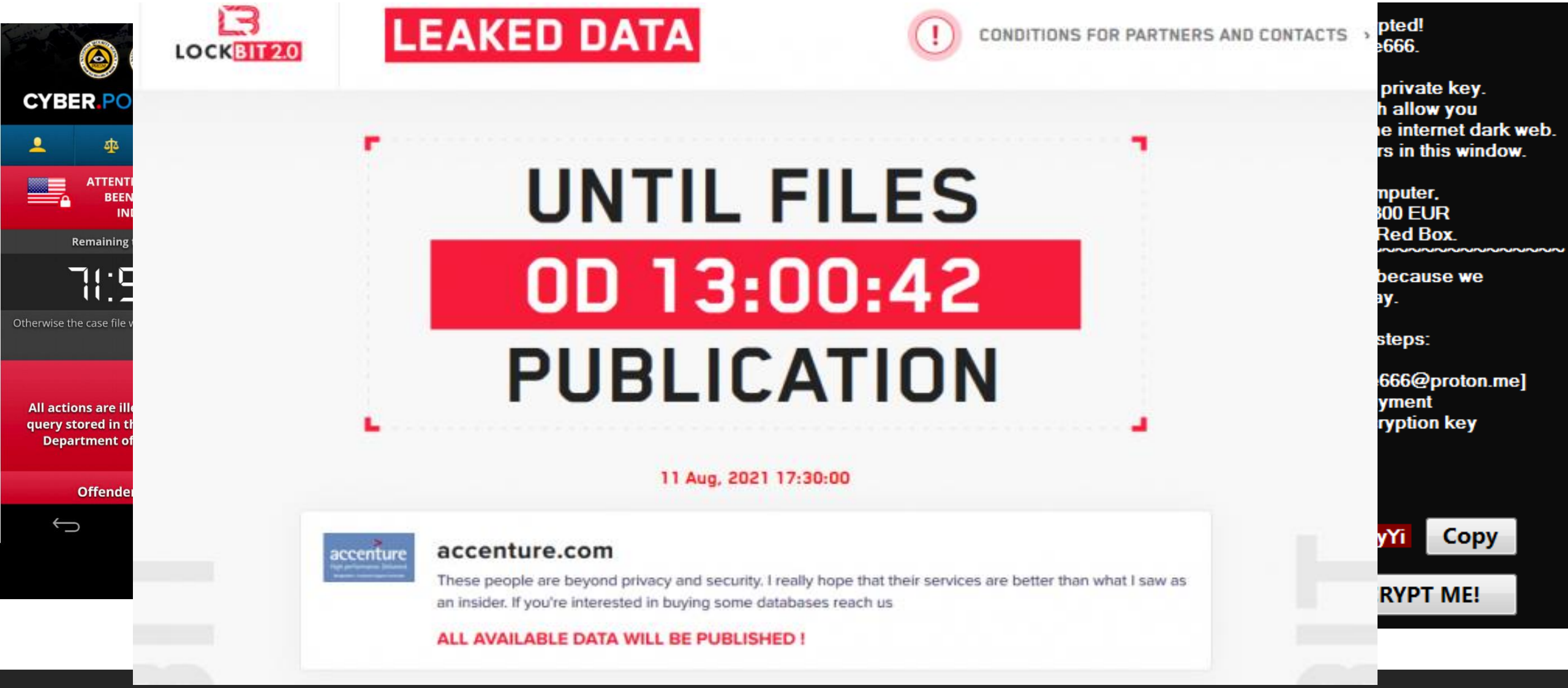
Ransomware as-a-service (RaaS)

Rápida Incorporação de Zero Days

Access as a Service (AaaS)

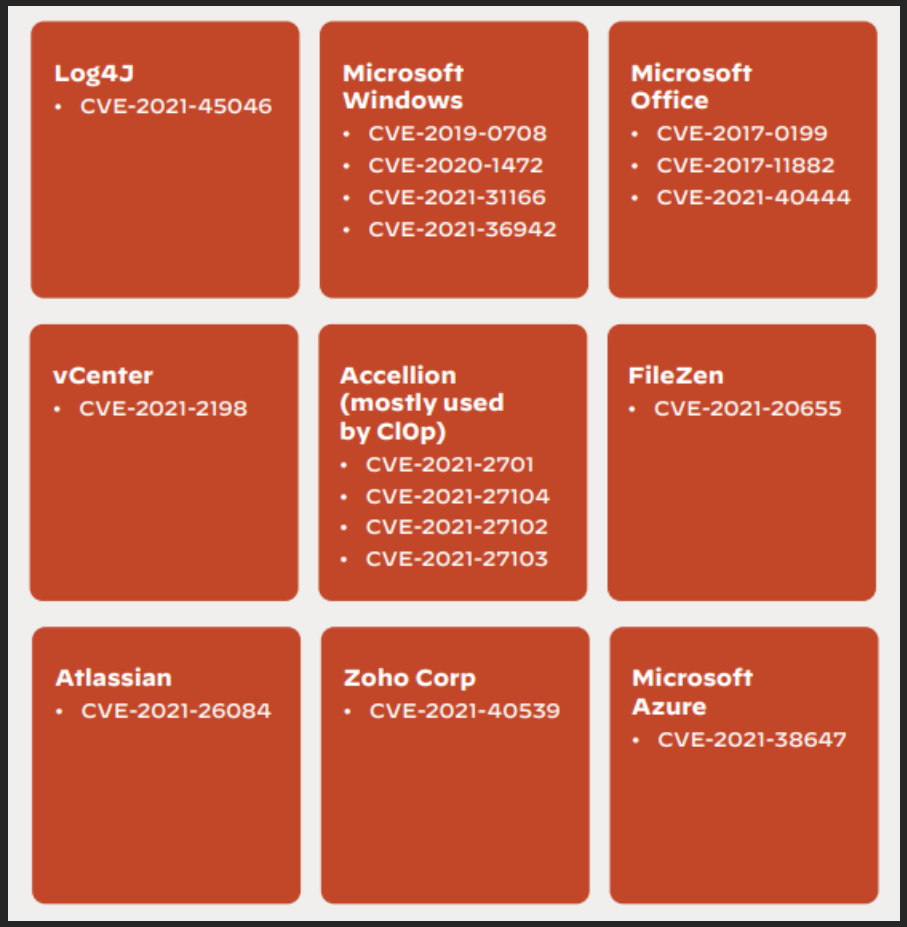
[4] UNIT 42 Ransomware Threat Report 2022

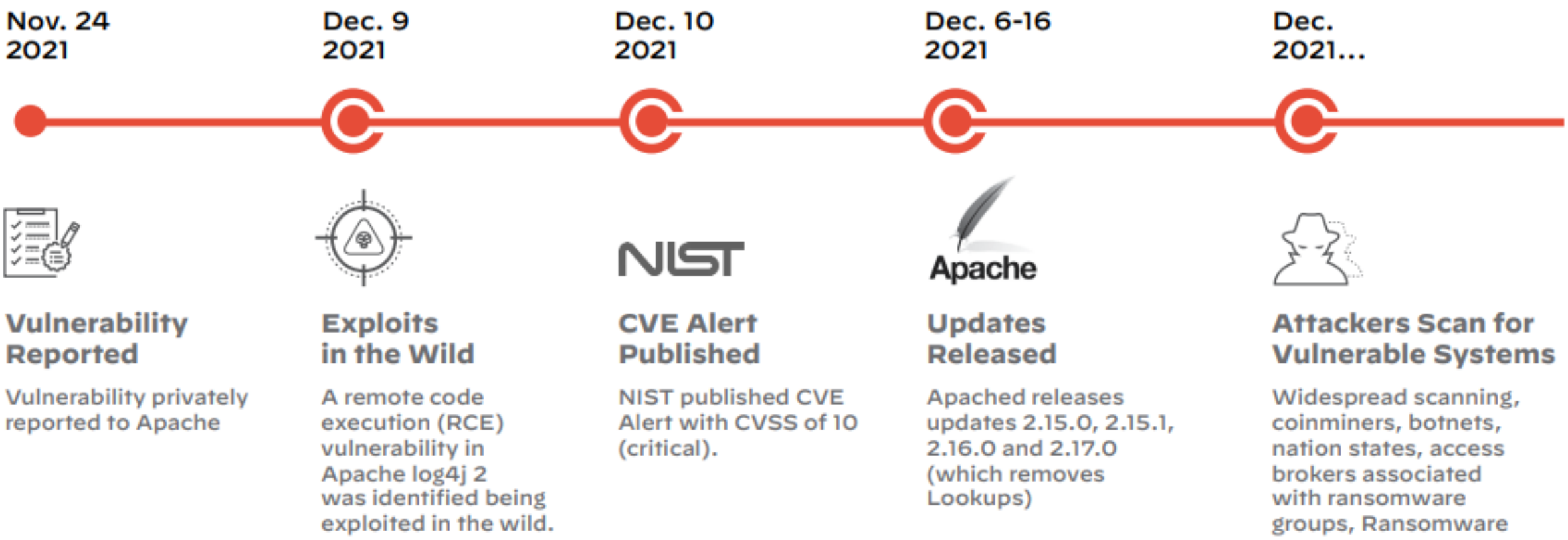
Exemplos de *Splash Screen* de Ransomware



Vulnerabilidades Exploradas por Ransomware em 2021

[4] UNIT 42 Ransomware Threat Report 2022





Weaponization do Log4j

[4] UNIT 42 RANSOMWARE THREAT REPORT 2022

Quem é o meu Adversário?

Vs.

Oportunístico

- Ataca muitos, indiscriminadamente
- Truques velhos e conhecidos
- Muitas vítimas e baixo valor de resgate
- Raramente furtivos, velocidade é a chave
- Baixo orçamento e pouca organização

Direcionado

- Ataca poucos, seleciona seus alvos
- Truques novos e inovadores, até inéditos
- Poucas vítimas, alto valor de resgate
- Lento, furtivo, se adapta a rede invadida
- Mais (muito mais) financiado e organizado.

Vetores Iniciais de Ataque

De acordo com as descobertas do DBIR 2022, podemos observar que os vetores iniciais de ataque mudam muito pouco com o passar do tempo.

40% RDP and Desktop Sharing
35% Phishing / Spearphishing
15% Web Application Exploitation
10% Direct Install / Insiders / Other

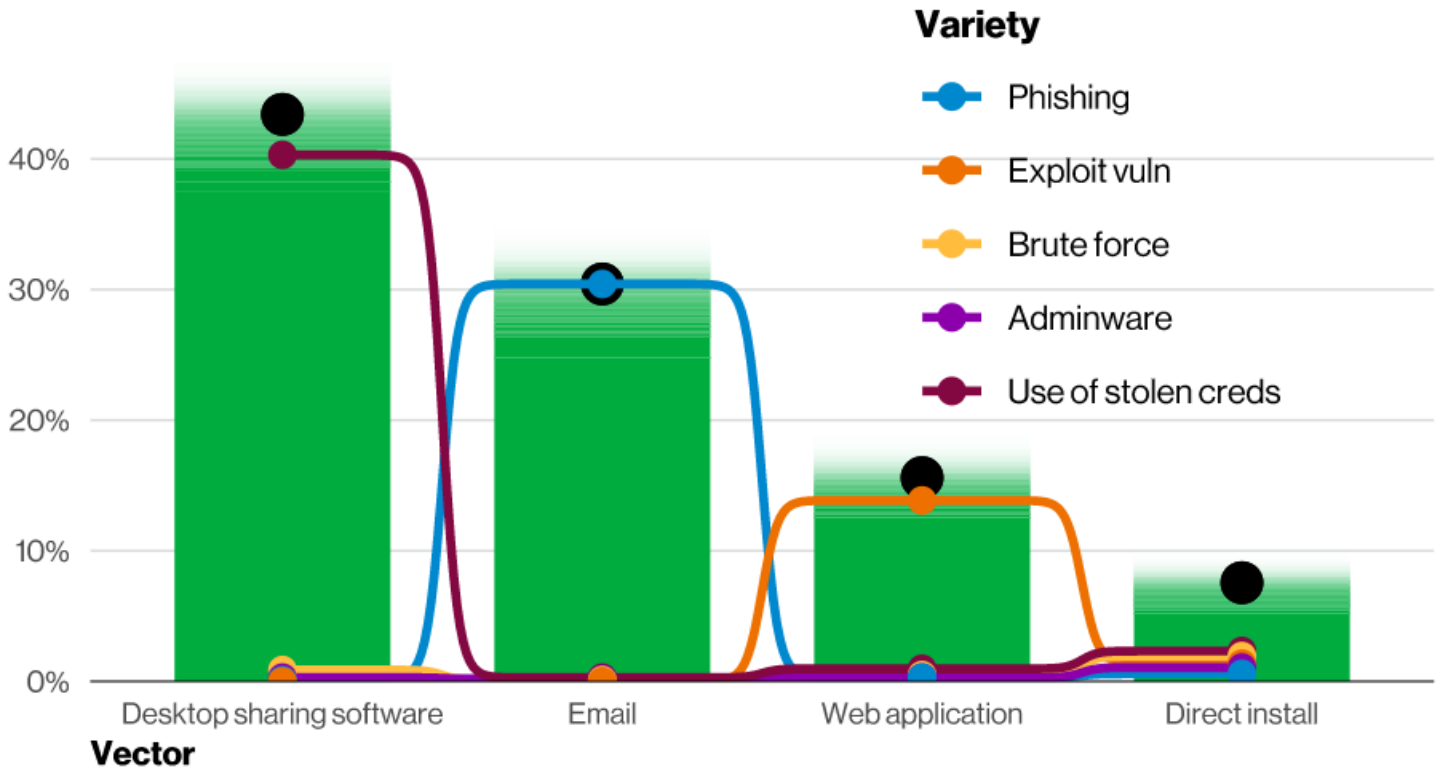
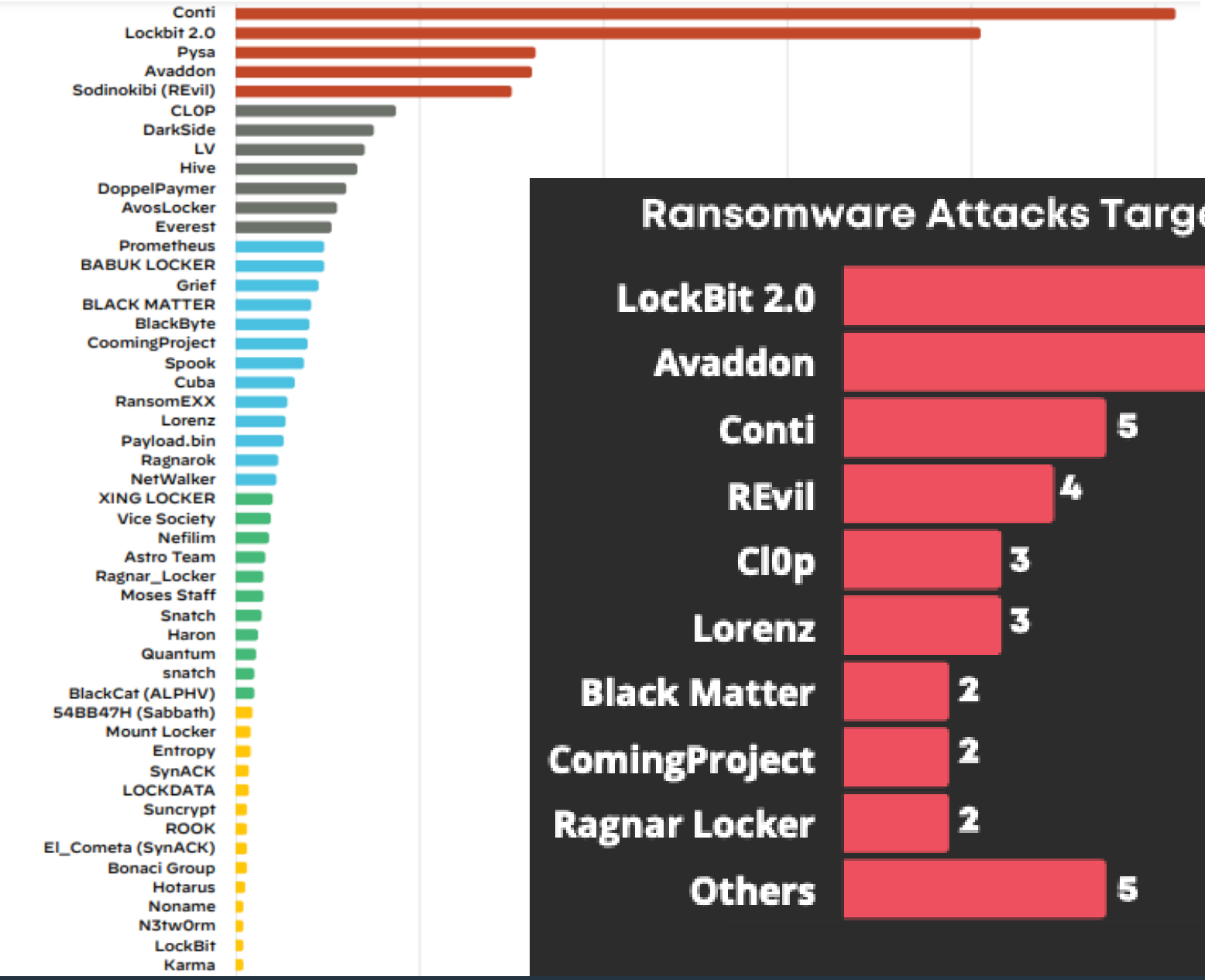
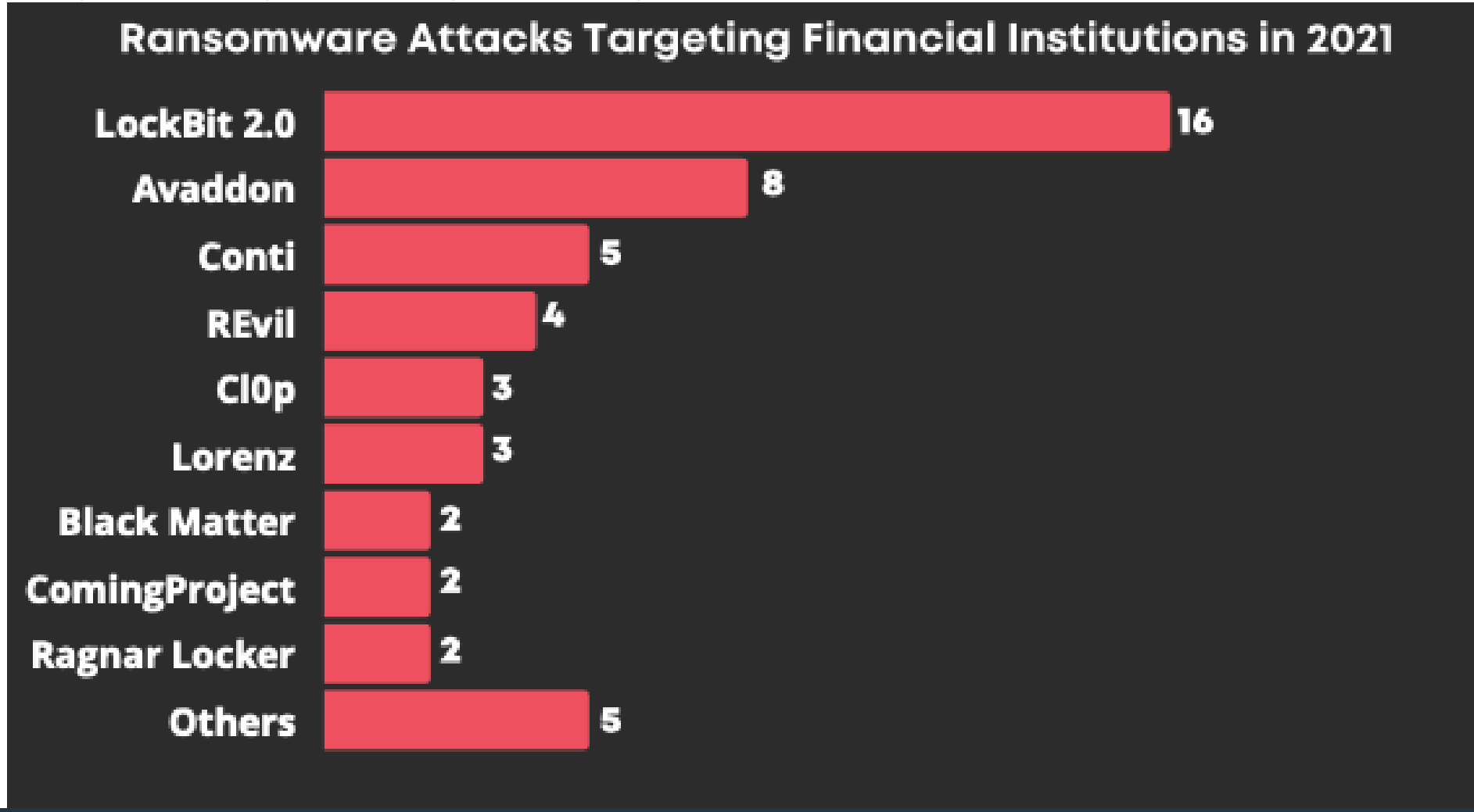


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

Ransomware é um modelo de monetização do acesso de uma organização comprometida que se tornou popular e veio para ficar enquanto for economicamente favorável aos invasores. Verizon DBIR 2022 [5]

Contagem de Vítimas por Grupos de Ransomware em 2021 [4]





O recorte entre o geral e o setor financeiro é ligeiramente diferente, o que mostra que uma abordagem Top 5 ou Top 10 irá nos fazer ignorar importantes variações desta ameaça. [6]

Detecção de Ransomware

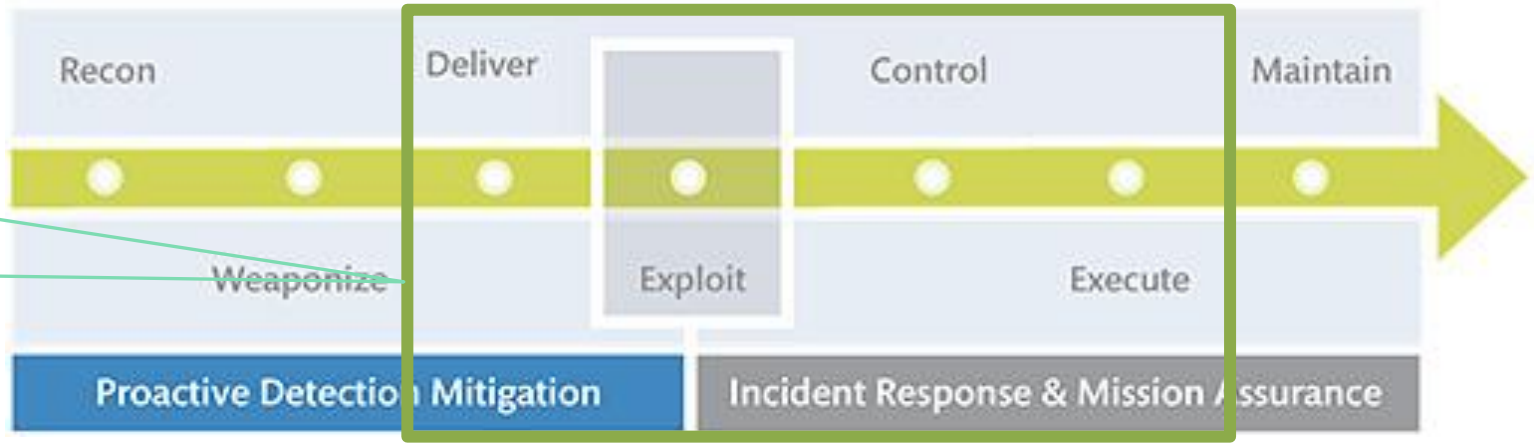
UMA ABORDAGEM AGNÓSTICA DE GRUPOS DE RANSOMWARE E SEUS IOCS

Threat Informed Defense - MITRE

A defesa baseada em ameaças [7] se utiliza do conhecimento ganho sobre os atacantes e seus métodos para reduzir a probabilidade ou impacto de futuros ataques bem sucedidos.

1. Análise da inteligência de ameaças
2. Engajamento defensivo da ameaça
3. Compartilhar e trocar informações de ameaças

Foco em detectar a ação da ameaça o quanto antes possível!



Comprometimento (IOCs) versus Ataque (IOAs)

O NIST SP 800-150 [8] define indicador como *Um artefato técnico ou observável que sugere que um ataque é iminente ou está em andamento, ou que um comprometimento já pode ter ocorrido.*

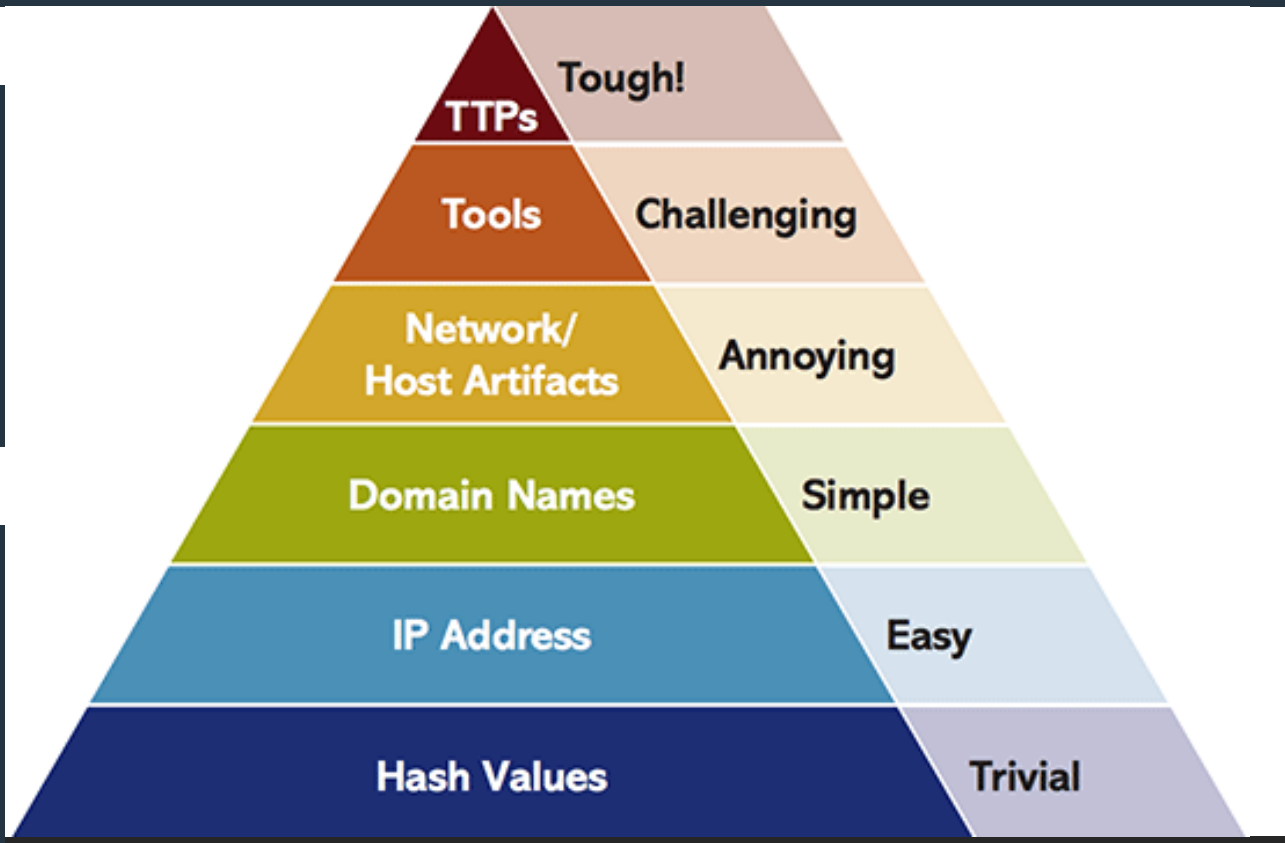
IOCs focam apenas no passado, IOAs são menos voláteis e mais abrangentes!

Detecção Agnóstica

Agnóstico, em um contexto de tecnologia da informação (TI), refere-se a algo que é generalizado para que seja interoperável entre vários sistemas. O termo pode se referir a software e hardware, bem como a processos ou práticas de negócios. [9]

Nosso foco deve ser em detecções robustas e de difícil evasão (IOAs e anomalias) de acordo com as fontes de detecção disponíveis.

Uma detecção agnóstica é aquela focada em comportamento potencialmente malicioso (IOAs) e não somente em IOCs de um grupo de ransomware específico.



Espectro Detectivo

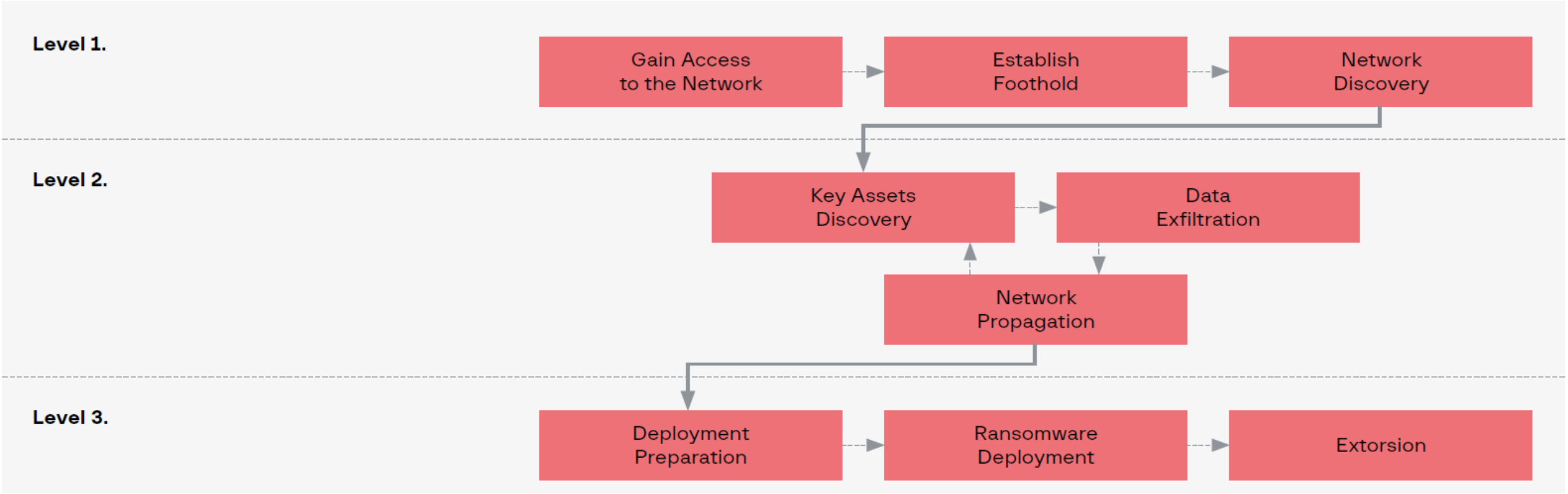
Toda as detecções recarem dentro do "espectro de detecção", onde uma extremidade representa a lógica "precisa", enquanto a outra representa a lógica "ampla". [10]

Precisa
Baixo FP
Alto FN

Gestão de riscos é fundamental,
não existe uma detecção bala de prata!

Ampla
Baixo FN
Alto FP

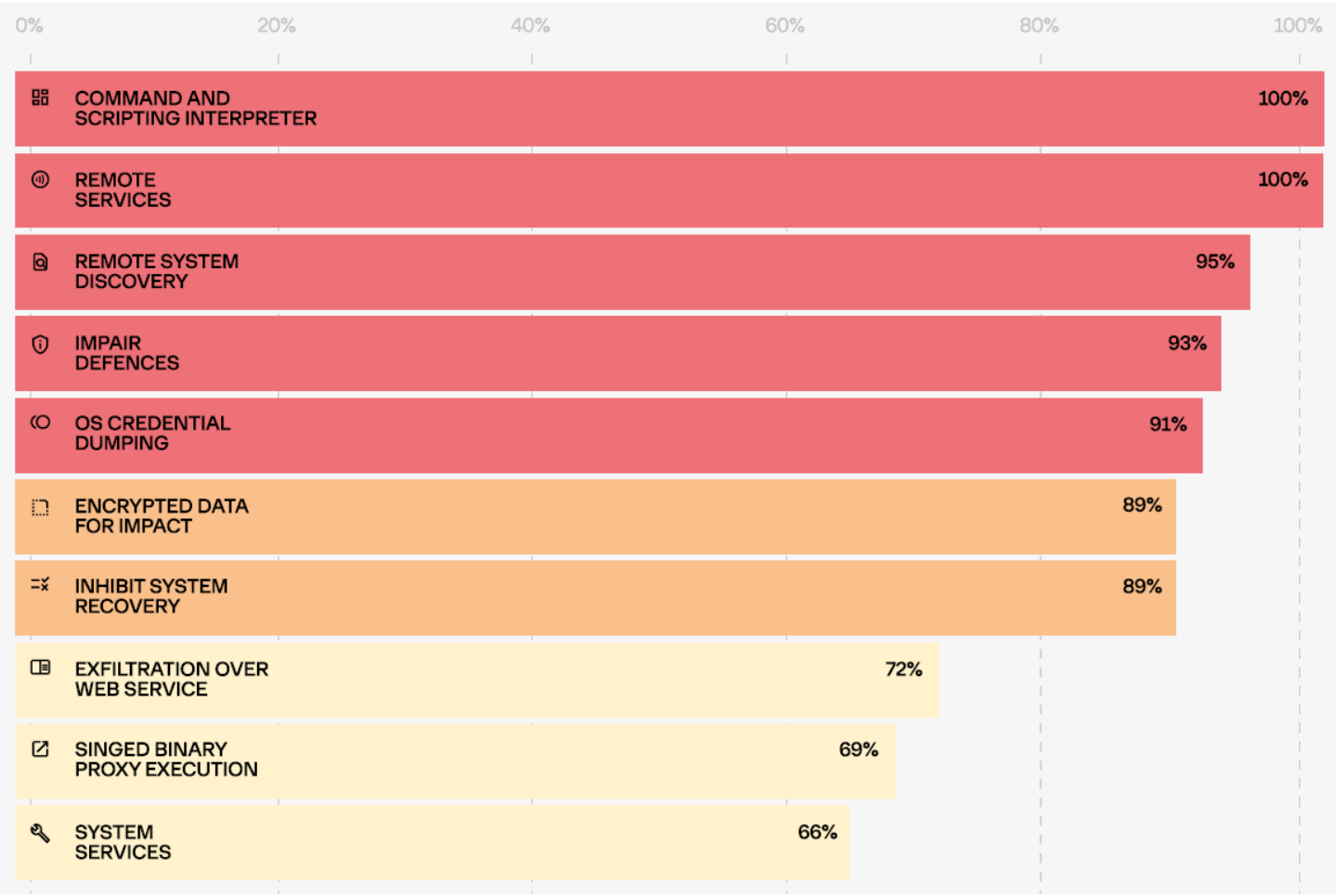
Como engenheiros de detecção, somos responsáveis por entender a amplitude da técnica ofensiva e o nível dos recursos de triagem e investigação de nossa organização para produzirmos detectores úteis!



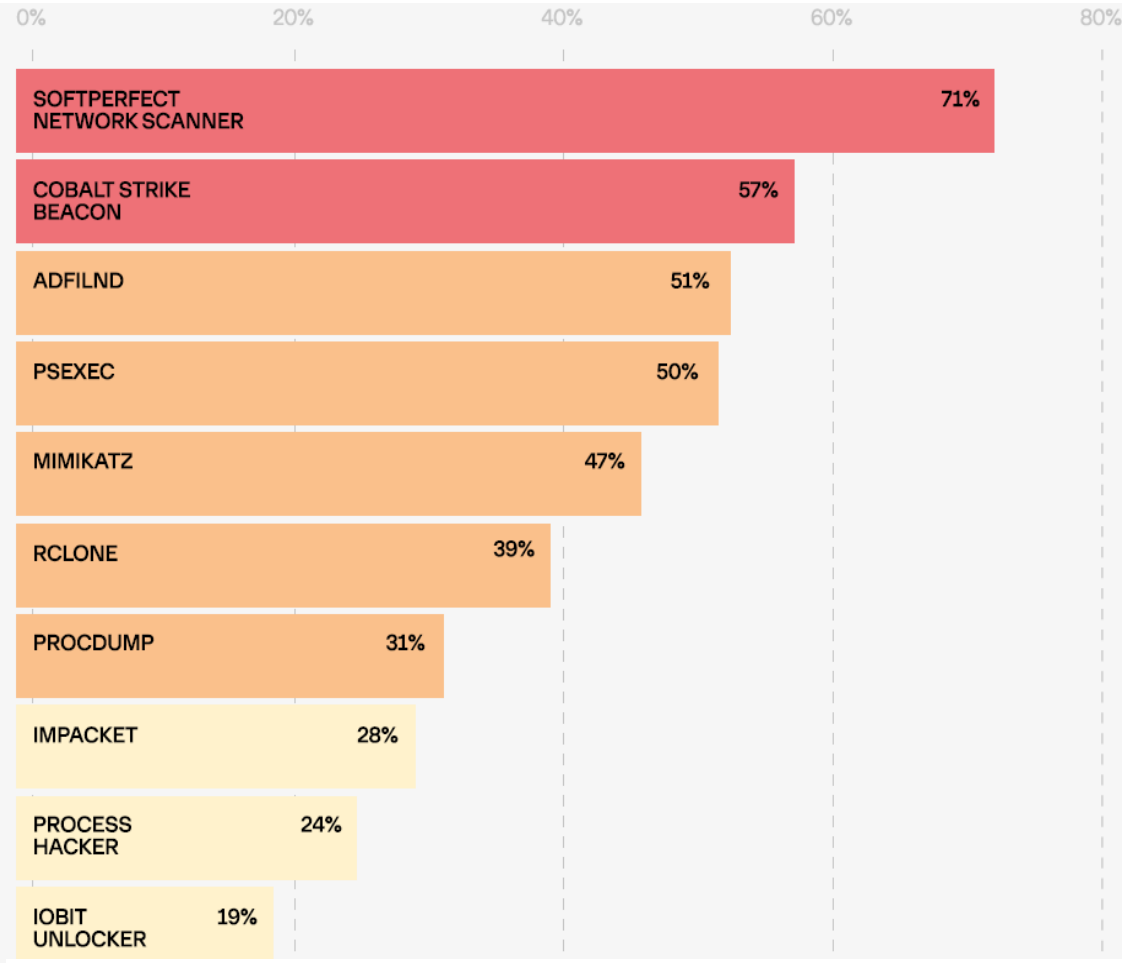
Ransomware Kill Chain

[11] GROUP-IB RANSOMWARE UNCOVERED 2021/2022 REPORT

Priorização de TTPs – Top 10 2021/2022



Top 10 técnicas usadas por grupos de ransomware

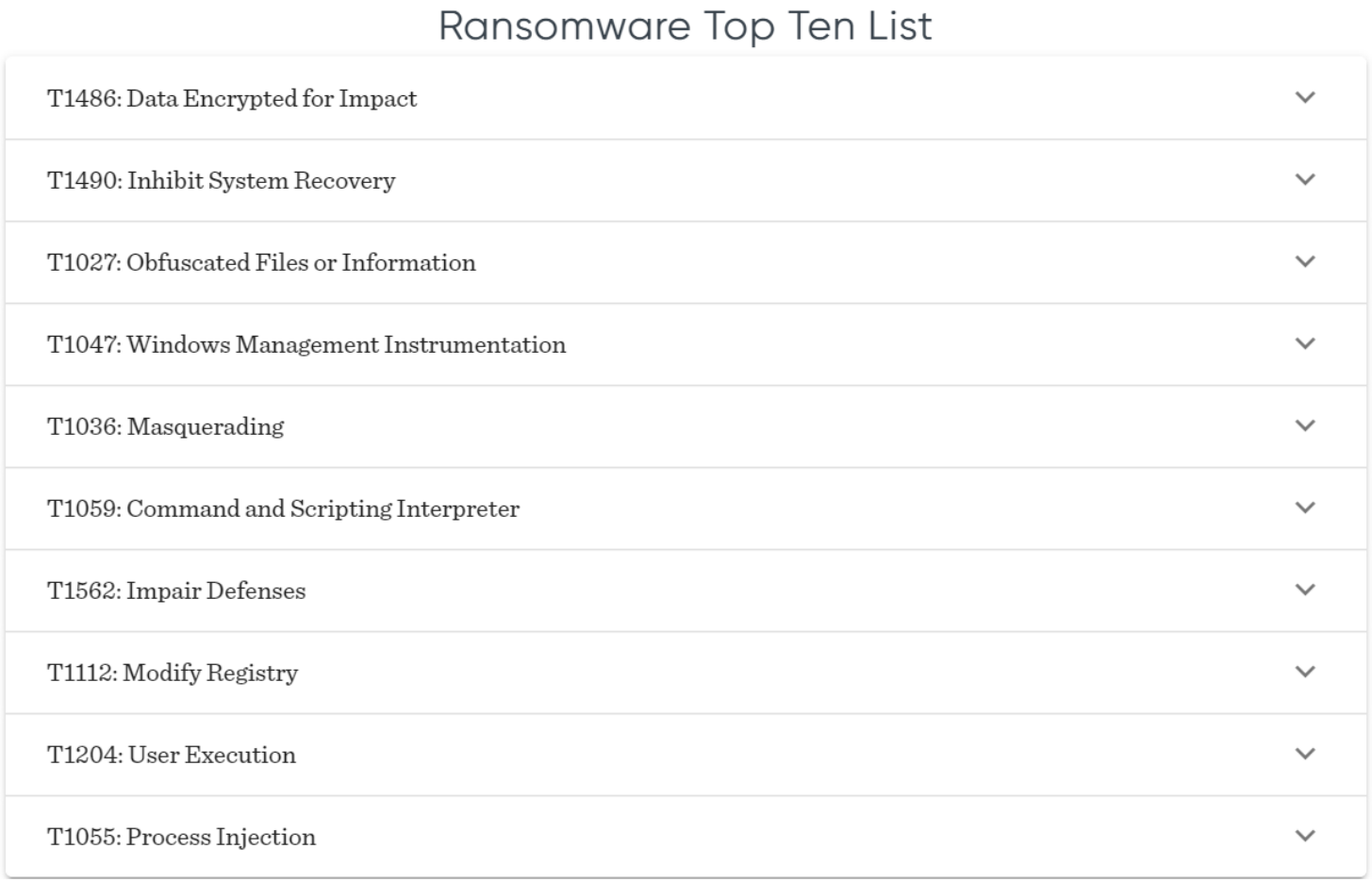


Top 10 ferramentas usadas por grupos de ransomware

MITRE ATT&CK® for ransomware operators in 2021/2022

Initial Access 1	External Remote Services T1133	Exploit Public-Facing Application T1190	Phishing T1566	Drive-by Compromise T1189	Hardware additions T1200	Supply Chain Compromise T1195												
Execution 2	Command and Scripting Interpreter T1059	Exploitation for Client Execution T1203	Native API T1106	Scheduled Task/Job T1053	Software Deployment Tools T1072	System Services T1569	User Execution T1204	Windows Management Instrumentation T1047										
Persistence 3	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Create Account T1136	External Remote Services T1133	Scheduled Task T1053	Server Software Component T1505	Valid Accounts T1078											
Privilege Escalation 4	Abuse Elevation Control Mechanism T1548	Access Token Manipulation T1134	Create or Modify System Process T1543	Exploitation for Privilege Escalation T1068	Hijack Execution Flow T1574	Process Injection T1055	Scheduled Task/Job T1053											
Defense Evasion 5	BITS Jobs T1197	Deobfuscate/ Decode Files or Information T1140	File and Directory Permissions Modification T1222	Hide Artifacts T1564	Impair Defenses T1562	Indicator Removal on Host T1070	Masquerading T1036	Obfuscated Files or Information T1027	Signed Binary Proxy Execution T1218	Subvert Trust Controls T1553	Virtualization/ Sandbox Evasions T1497							
Credential Access 6	OS Credential Dumping T1003	Brute Force T1110	Credentials from Password Stores T1555	Exploitation for Credential Access T1212	Unsecured Credentials T1552	Steal or Forge Kerberos Tickets T1558	Input Capture T1056											
Discovery 7	Account Discovery: Local Account T1087.001	Account Discovery: Domain Accounts T1087.002	Permission Groups Discovery: Local Groups T1069.001	Permission Groups Discovery: Domain Groups T1069.002	Domain Trust Discovery T1482	Remote System Discovery T1018	Network Service Scanning T1046	Network Share Discovery T1135	System Network Connections Discovery T1049	System Network Configuration Discovery T1016	System Information Discovery T1082	System Owner/User Discovery T1033	Software Discovery T1518	Process Discovery T1057	System Service Discovery T1007	File and Directory Discovery T1083	Query Registry T1012	Software Discovery: Security Software Discovery T1518.001
Lateral Movement 8	Exploitation of Remote Services T1210	Remote Services: Remote Desktop Protocol T1021.001	Remote Services: SMB/Windows Admin Shares T1021.002	Valid Accounts: Domain Accounts T1078.002	Valid Accounts: Local Accounts T1078.003	Lateral Tool Transfer T1570	Use Alternate Authentication Material T1550	Internal Spearphishing T1534	Phishing T1566	Distributed Component Object Model T1021.003	Windows Remote Management T1021.006	Pass the Ticket T1550.003	Software Deployment Tools T1072					
Collection 9	Archive Collected Data T1560	Automated collection T1119	Data from Local System T1005	Data from Network Shared Drive T1039														
Command and Control 10	Application Layer Protocol T1071	Encrypted channel T1573	Data encoding T1132	Data Obfuscation T1001	Fallback Channels T1008	Multi-Stage Channels T1104	Ingress Tool Transfer T1105	Protocol Tunneling T1572	Proxy T1090	Remote Access Software T1219								
Exfiltration 11	Data transfer limits T1030	Exfiltration Over Web Service T1567	Automated Exfiltration T1020															
Impact 12	Inhibit System Recovery T1490	Data Destruction T1485	Data Encrypted for Impact T1486															

Priorização de TTPs – MITRE CTID

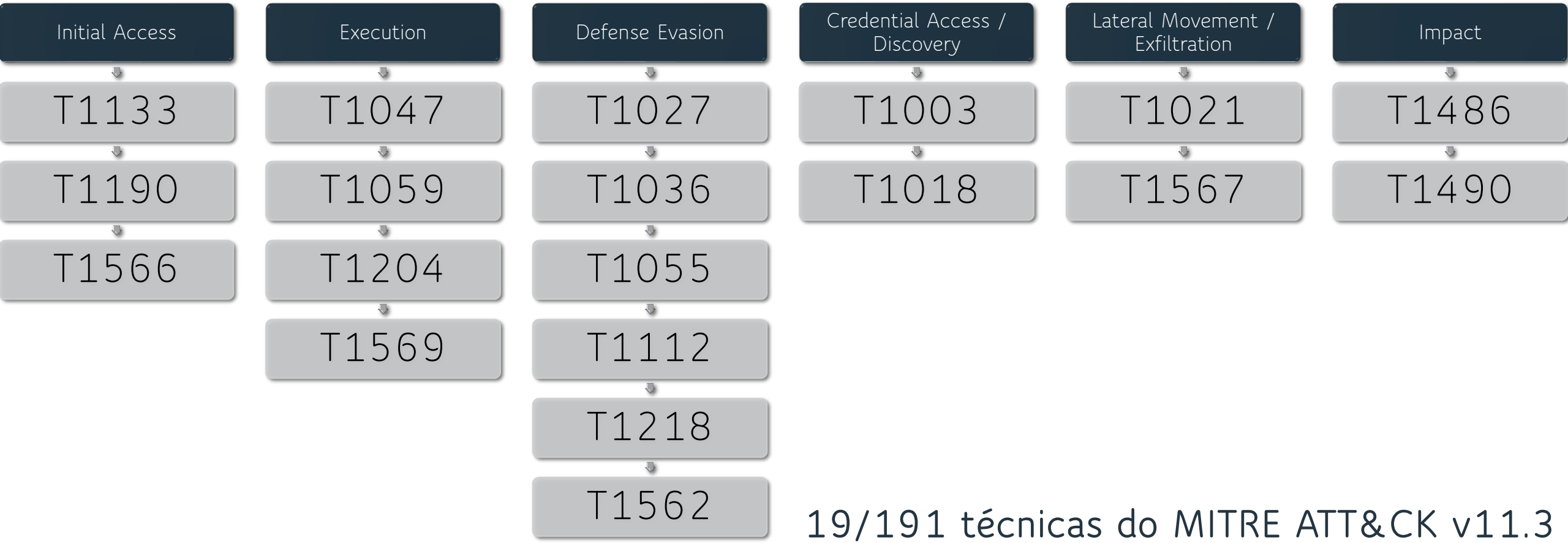


A partir de uma análise de 22 grupos de ransomware nos últimos três anos, o **Center for Threat-Informed Defense** criou uma lista das 10 principais técnicas ATT&CK para ransomware [12].

É um ponto de partida para priorizar as principais técnicas para se defender contra ataques de ransomware, embora não considere vetores de entrada iniciais como a Verizon faz.

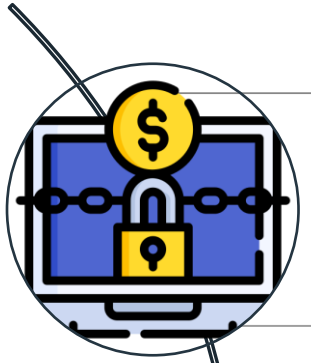
Priorização de TTPs – Consolidação

A compreensão holística de uma ameaça nos permite priorizar a detecção de técnicas do ATT&CK

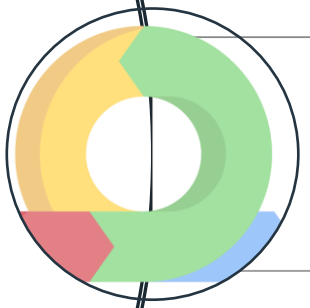


19/191 técnicas do MITRE ATT&CK v11.3

Conclusão



Atores de ameaça que se valem do uso de ransomware estão melhorando constantemente e isso não deve parar



Blue Teams precisam ser ágeis e devem incorporar constantemente inteligência de ameaças em seus controles de segurança

Parar/Detectar a ameaça numa fase inicial é fundamental, aumentando ao máximo o custo do ataque para um adversário.

Referências I

[1] M-trends 2022 - https://www.mandiant.com/media/15671

[2] Webroot Report - https://mypage.webroot.com/rs/557-FSI-195/images/21Q3_C%2BW_Chapter%201_Ransomware_EB.pdf

[3] The Industries Most Affected by Ransomware - https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/

73 Ransomware Statistics Vital for Security in 2022 - https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/

86 Ransomware Statistics, Data, Trends, and Facts [updated 2022] -https://www.varonis.com/blog/ransomware-statistics

Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021 - https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021

[4] UNIT 42 Ransomware Threat Report 2022 - https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf

Referências II

[5] Verizon DBIR 2022 https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-intro-to-patterns/

[6] Around 50 Ransomware Attacks Targeting Financial Institutions -https://socradar.io/around-50-ransomware-attacks-targeting-financial-institutions/

[7] Threat Based Defense - https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

[8] NIST Special Publication 800-150 - Guide to CTI Sharing - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[9] Agnostic in IT - https://www.techtarget.com/whatis/definition/agnostic

[10] Detection Spectrum - https://posts.specterops.io/detection-spectrum-198a0bfb9302

[11] Group-IB Ransomware Uncovered 2021/2022 report - https://www.group-ib.com/resources/threat-research/ransomware-2022.html

[12] Top 10 ATT&CK Techniques list for ransomware - https://top-attack-techniques.mitre-engenuity.org/

Perguntas são muito bem-vindas!

MUITO OBRIGADO PELA OPORTUNIDADE!