The Evolution of Ransomware

From Malware to Sophisticated Cyber Operations

About Me

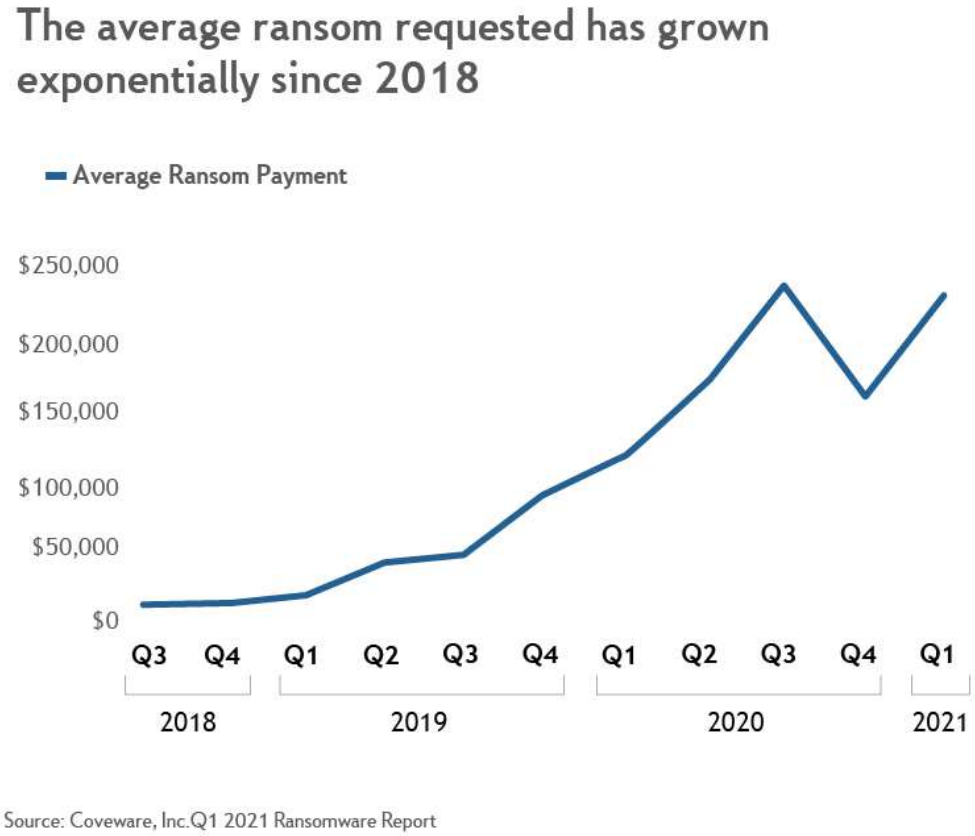
- Florian Roth
- Head of Research @ Nextron Systems
- Timeline
  - seit 2000: IT Security - Security Monitoring
  - seit 2012: Cyber Wirtschaftsspionage
  - seit 2017: Nextron Systems
- Twitter @cyb3rops
- Open-Source Projekte wie z.B. Sigma
- Link Tree: https://linktr.ee/cyb3rops

nextron systems

1. The Evolution of Ransomware
2. Increasing Resistance
3. Let’s talk about Resilience

Ransomware: Eine moderne Epidemie

- **Nie dagewesenes Wachstum**
  - Unternehmen auf der ganzen Welt betroffen
  - 68% aller Cyber Angriffe
- **Eskalierende Bedrohungen**
  Zunehmend ausgefeiltere und schneller ablaufende Angriffe
  - “dwell time“:
    von 9 Tagen in 2022 zu 5 Tagen in 2023
- **Finanzielle Auswirkungen**
  Lösegelder in Milliardenhöhe und zusätzliche Kosten
  - Betriebsausfälle werden oft vergessen



Cyberkriminalität vor der Ransomware-Ära

1. **Identitäts- und Informationsdiebstahl**
   Cyberkriminelle nutzen verschiedene Methoden, darunter **Banking-Trojaner** und Phishing-Betrug, um persönliche und finanzielle Informationen zu stehlen. Die gestohlenen Informationen werden für nicht genehmigte Transaktionen, Kreditanträge und andere betrügerische Handlungen verwendet. Informationen wie **Kreditkartendetails**, Anmeldedaten und andere sensible Daten werden auf Untergrundmärkten verkauft.
2. **Phishing-Betrügereien**
   E-Mails oder Nachrichten, die den Empfänger dazu verleiten sollen, vertrauliche Informationen wie Passwörter oder Kreditkartennummern preiszugeben.
3. **Anzeigenbetrug**
   Betrügerische Manipulation von Online-Werbeprozessen zur Erzielung von Einnahmen, einschließlich Klickbetrug und Display-Ad-Betrug.
4. **Botnets zum Mieten**
   Cyberkriminelle vermieten den Zugang zu Netzwerken kompromittierter Computer (Botnets) an andere für Spam-

Die Historische Entwicklung

- **Konzeptionelle Wurzeln (1980er Jahre)**
  - 1986: Dr. Joseph Popp entwickelt den AIDS-Trojaner (auch bekannt als PC Cyborg). Er gilt als die erste Ransomware. Er verschlüsselte Dateinamen auf dem Computer des Opfers und forderte eine Zahlung zur "Erneuerung der Lizenz".
- **Entwicklung (1990er - Anfang 2000er)**
  - In diesem Zeitraum gab es nur begrenzte Ransomware-Aktivitäten, was in erster Linie auf das Fehlen eines weit verbreiteten Internetzugangs und moderner Zahlungsplattformen zurückzuführen ist.
  - Einige Ransomware-Programme setzten eher auf Social Engineering als auf Verschlüsselung. Die "polizeiliche" Ransomware zum Beispiel teilte den Opfern mit, sie hätten gegen das Gesetz verstoßen und müssten eine Geldstrafe zahlen.
- **Aufkommen der Verschlüsselung (Ende 2000er)**
  - 2005: Archiveus war einer der ersten Ransomware-Stämme, der RSA-Verschlüsselung verwendete. Er sperrte Dateien in einer passwortgeschützten ZIP-Datei.
  - 2007: Die WinLock-Ransomware taucht auf. Sie verschlüsselte keine Dateien, sondern sperrte die Benutzer von ihren Desktops aus, zeigte pornografische Bilder an und verlangte eine Premium-SMS zum Entsperren.

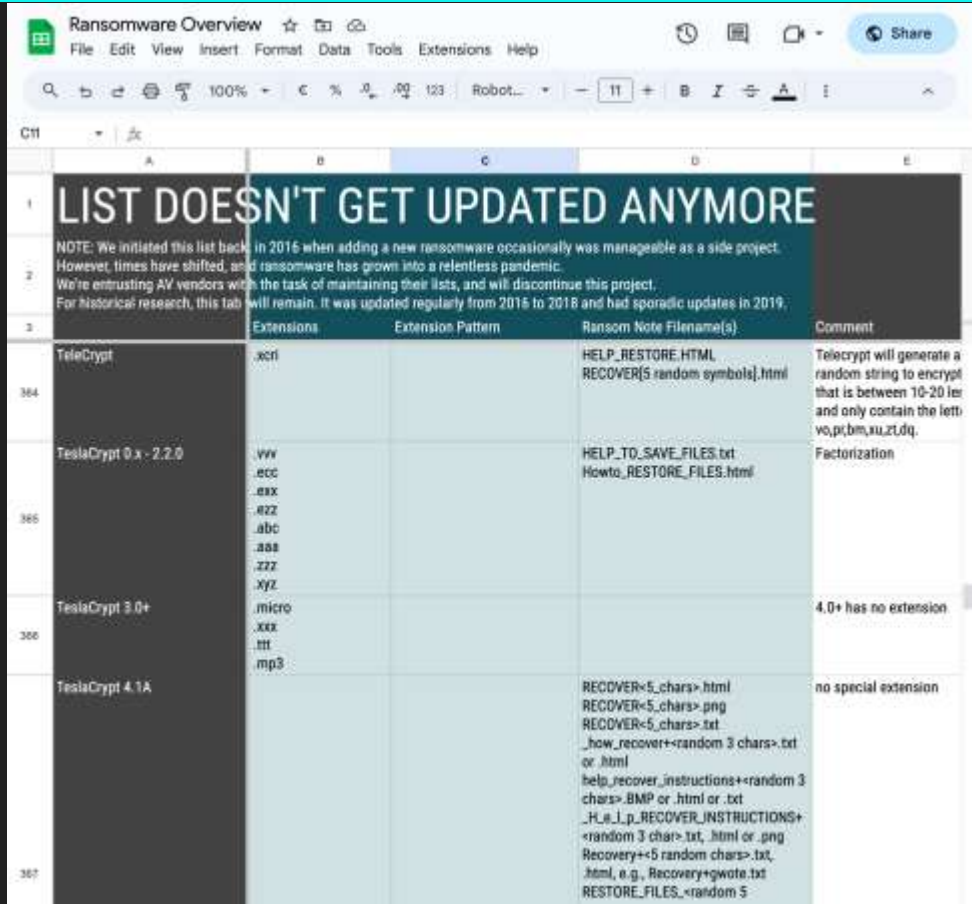
Was hat sich geändert?

Warum wurde Erpressung so populär?

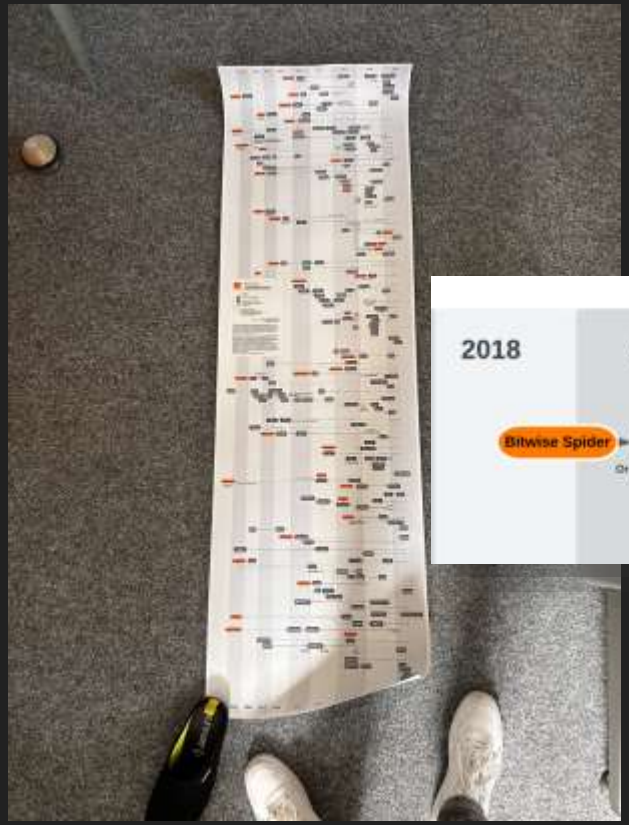
- **Krypto-Währungen:** Anonymität und Überweisungen ohne Limit
- **Dark Web:** Zugang über das Tor-Netzwerk (TOX Chats)
- **Cyber-Versicherungen:** Decken oft Lösegeldzahlungen ab
- **Remote Work:** Vergrößerte Angriffsfläche

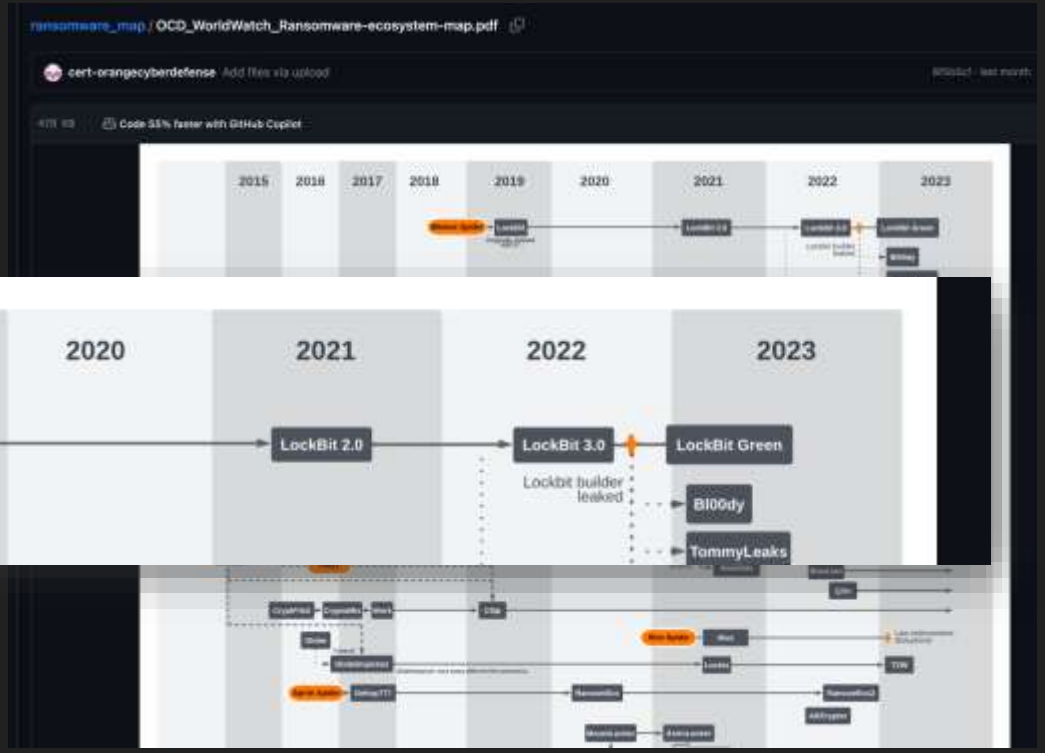
Explosionsartiges Wachstum der Ransomware-Gruppen

- Mein öffentliches Google Spreadsheet aus dem Jahr 2016



Explosionsartiges Wachstum der Ransomware-Gruppen

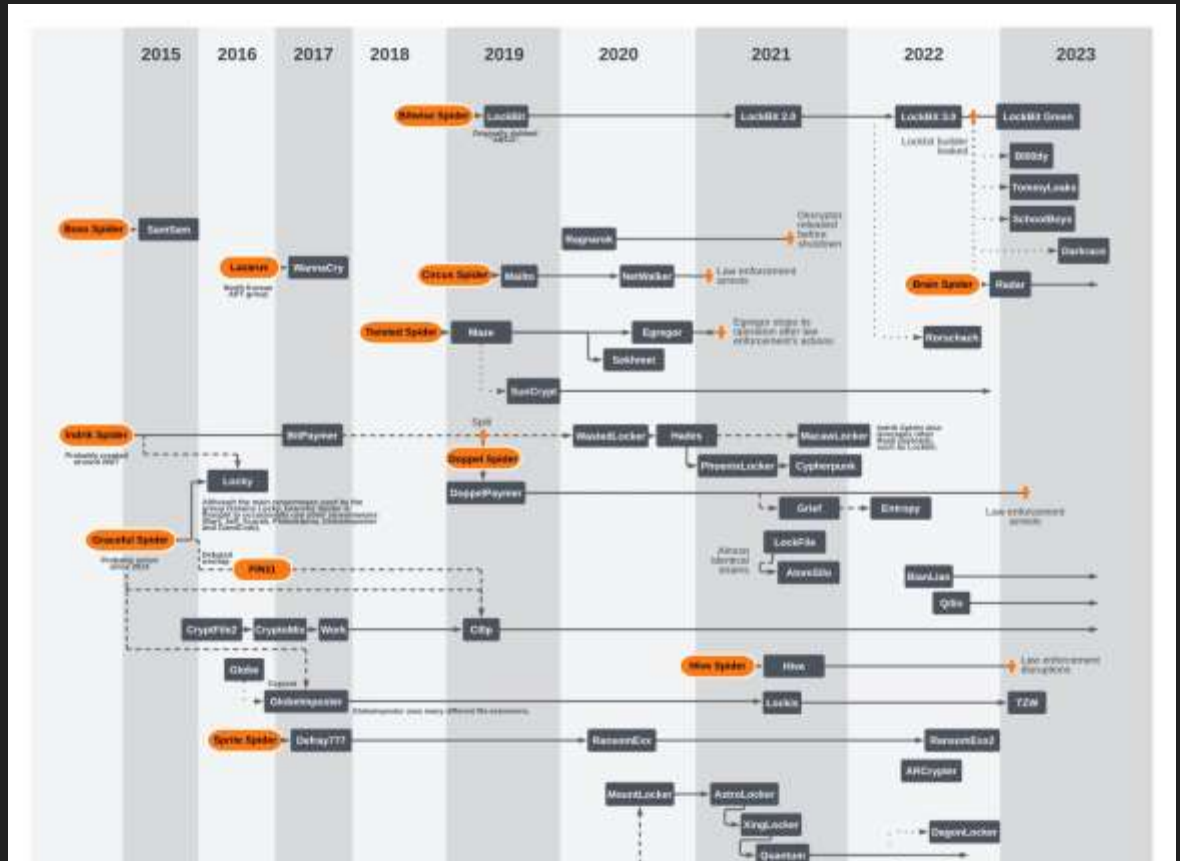




Source: Orange Cyber Defense https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf

Explosionsartiges Wachstum der Ransomware-Gruppen

Orange Cyberdefense
“Ransomware Ecosystem Map”



Die Evolution von Ransomware: Ein zeitlicher Überblick

	Die frühen Jahre (*-2016)	Reifephase (2016-2020)	Heute (2020-*)
Ransomware ist	Nur eine Art von Malware		
Beteiligte	Malware-Entwickler		
Ziele	Hauptsächlich Einzelpersonen		
Vorgehensweise	Automatisch		
Auswirkungen	Einzelne Systeme		
Bedrohung	Leere Drohungen, Verschlüsselung		
Zahlungsarten	PaySafe, SMS zum Premium-Tarif, Überweisungsdienste		
Lösegeldbeträge	Niedrig (fest; normalerweise $100-$500)		

Die Evolution von Ransomware: Ein zeitlicher Überblick

	Die frühen Jahre (*-2016)	Reifephase (2016-2020)	Heute (2020-*)
Ransomware ist	Nur eine Art von Malware	Automatisch oder manuell installierte Malware	
Beteiligte	Malware-Entwickler	Access Broker, Malware-Entwickler, Support Mitarbeiter	
Ziele	Hauptsächlich Einzelpersonen	Unternehmen, KMUs, Behörden und Privatpersonen	
Vorgehensweise	Automatisch	Mischung aus automatisch und manuell	
Auswirkungen	Einzelne Systeme	**Windows-Umgebung (AD)**	
Bedrohung	Leere Drohungen, Verschlüsselung	Verschlüsselung	
Zahlungsarten	PaySafe, SMS zum Premium-Tarif, Überweisungsdienste	Überweisungen in Kryptowährung (BTC, XMR)	
Lösegeldbeträge	Niedrig (fest; normalerweise $100-$500)	Hoch (oft abhängig von der Größe des Opfers)	

Die Evolution von Ransomware: Ein zeitlicher Überblick

	Die frühen Jahre (*-2016)	Reifephase (2016-2020)	Heute (2020-*)
Ransomware ist	Nur eine Art von Malware	Automatisch oder manuell installierte Malware	Letzte Stufe bei einem **mehrstufigen Angriff**
Beteiligte	Malware-Entwickler	Access Broker, Malware-Entwickler, Support Mitarbeiter	Access Broker, Malware-Entwickler, RaaS-Partner, RaaS-Betreiber, Support Mitarbeiter, Web Entwickler
Ziele	Hauptsächlich Einzelpersonen	Unternehmen, KMUs, Behörden und Privatpersonen	**Überwiegend Unternehmen**, KMUs und Behörden
Vorgehensweise	Automatisch	Mischung aus automatisch und manuell	**Vor allem manuell** und massenhafte Ausnutzung von Schwachstellen
Auswirkungen	Einzelne Systeme	**Windows-Umgebung (AD)**	**Hypervisors (mit Auswirkungen auf alle VMs), Speicher (einschließlich Backups)**
Bedrohung	Leere Drohungen, Verschlüsselung	Verschlüsselung	Verschlüsselung, **Exfiltration, Erpressung**
Zahlungsarten	PaySafe, SMS zum Premium-Tarif, Überweisungsdienste	Überweisungen in Kryptowährung (BTC, XMR)	Überweisungen in Kryptowährungen (BTC, XMR, ETH, Dash, ZEC)
Lösegeldbeträge	Niedrig (fest; normalerweise $100-	Hoch (oft abhängig von der Größe des	Hoch (auf die finanzielle Situation

Was liegt vor uns?

- Exfiltration und Erpressung nehmen zu
  - Backups werden Sie nicht retten
- Legitime Werkzeuge für Angriffe
  - Weniger Malware, stattdessen legitime Remote-Zugriffs- und Verschlüsselungs-Software > Baselining erforderlich
- Ransomware-freie Angriffe?
- Gray Zone Devices*
  - Netzwerkgeräte, Appliances und IOT Devices als Angriffsvektoren
  - Nicht durch Antivirus / EDR abgedeckt
- Gefährdete Cloud-Speicher
  - Angriffe über gestohlene Zugangsdaten
  - Daten werden gelöscht oder verschlüsselt

nextron systems

1. The Evolution of Ransomware
2. Increasing Resistence
3. Let’s talk about Resilience

Resistance

die Fähigkeit, von etwas nicht beeinträchtigt zu werden, insbesondere nicht nachteilig

Increasing Resistance

- Altes Slide-Deck von 2018
- Die alten empfohlenen Maßnahmen zur Erhöhung der Widerstandsfähigkeit sind im Grunde alle überholt

Entmystifizierung des Hypes

- Parallele Taktiken
  - Die Vorgehensweise moderner Ransomware Gruppen ähneln sehr stark den Methoden von Cyber Spionagegruppen
- Einziger Unterschied
  - Die Datenverschlüsselung und nachfolgenden Lösegeldforderungen
- Realitätscheck: Backups
  - Einzige spezifische Gegenmaßnahme
  - Allerdings nehmen Daten-Exfiltration und Expressung zu
  - Die Backups selbst stehen heute im Fokus > werden gelöscht oder verschlüsselt
  - Betrifft auch Cloud Backups oder Cold Backups

5 Wege, sich vor Ransomware-Angriffen zu schützen

Strategies Across the Kill Chain

	Entry	Infection	Propagation
Methods	Phishing Vulnerabilities Brute Force	Malicious Document Dropper/Downloader Manual Deployment	Network Scanning Extracted Credentials Exploitation
Detection			
Protection			
Resistance			
Resilience			

Strategies Across the Kill Chain

	Entry	Infection	Propagation
Methods	Phishing Vulnerabilities Brute Force	Malicious Document Dropper/Downloader Manual Deployment	Network Scanning Extracted Credentials Exploitation
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Protection	Multi-Factor-Authentication Email Filters	Antivirus / EDR	IPS
Resistance	Security Awareness Tranings Firewalling Patch Management	Policies Execution Prevention ASR	Firewalling Network Segregation User Account Segregation
Resilience	Entry Vector Discovery Backdoor Discovery Password Hygiene		

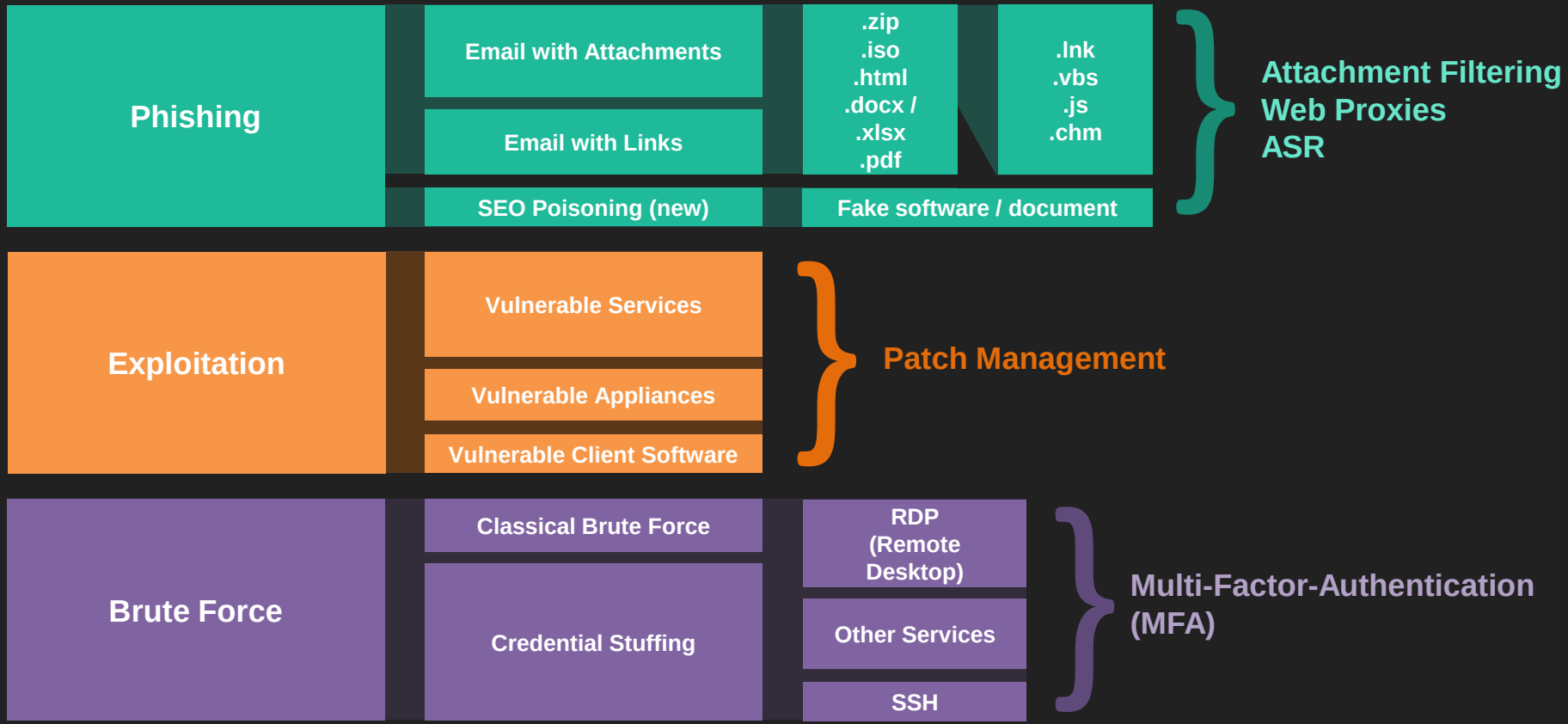
Strategies Across the Kill Chain

	Entry	Infection	Propagation
Methods	Phishing Vulnerabilities Brute Force	Malicious Document Dropper/Downloader Manual Deployment	Network Scanning Extracted Credentials Exploitation
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Protection	Multi-Factor-Authentication Email Filters	Antivirus / EDR	IPS
Resistance	Security Awareness Tranings Firewalling Patch Management	Policies Execution Prevention ASR	Firewalling Network Segregation User Account Segregation
Resilience	Entry Vector Discovery Backdoor Discovery Password Hygiene		

Strategies Across the Kill Chain

	Entry	Infection	Propagation
Methods	Phishing Vulnerabilities Brute Force	Malicious Document Dropper/Downloader Manual Deployment	Network Scanning Extracted Credentials Exploitation
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Protection	Multi-Factor-Authentication Email Filters	Antivirus / EDR	IPS
Resistance	Security Awareness Tranings Firewalling Patch Management	Policies Execution Prevention ASR	Firewalling Network Segregation User Account Segregation
Resilience	Entry Vector Discovery Backdoor Discovery Password Hygiene		

Typical Entry Vectors and Simple Counter Measures



nextron systems

1. The Evolution of Ransomware
2. Increasing Resistance
3. Let’s talk about Resilience

Resilience

die Fähigkeit, sich schnell von Schwierigkeiten zu erholen; Zähigkeit

Strategies Across the Kill Chain

	Entry	Infection	Propagation
Methods	Phishing Vulnerabilities Brute Force	Malicious Document Dropper/Downloader Manual Deployment	Network Scanning Extracted Credentials Exploitation
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Protection	Multi-Factor-Authentication Email Filters	Antivirus / EDR	IPS
Resistance	Security Awareness Tranings Firewalling Patch Management	Policies Execution Prevention ASR	Firewalling Network Segregation User Account Segregation
Resilience	Entry Vector Discovery Backdoor Discovery Password Hygiene		

Was denken Sie: Wie oft wiederholen sich Angriffe?

A) 10% B) 20% C) 30%

Was denken Sie: Wie oft wiederholen sich Angriffe?

A) 10% B) 20% C) 30% D) ~50%

Wiederholte Ransomware-Angriffe: Ursachen und Risiken

- ~50% der Opfer werden erneut erfolgreich angegriffen
- Die Gründe:
  - Forensik unvollständig
  - Nicht vollständige Behebung der Schwachstellen, die zu der ursprünglichen Kompromittierung geführt haben
  - Angreifer hinterlassen Backdoors
  - Passwort-Reset unvollständig
- Die Angreifer gehen davon aus, dass eine Organisation, die einmal ein Lösegeld gezahlt hat, bereit sein könnte, erneut zu

Welche Maßnahmen erhöhen die Resilienz?

- Digitale Forensik
  - Einstiegsvektor Entdeckung
- Patch Management
  - Identifizierung und Schließung von Schwachstellen
  - Patches für verwundbare Dienste oder Geräte
- Compromise Assessments
  - Backdoor-Entdeckung
- Security Monitoring
  - Überwachung auf ungewöhnliche Netzwerk- oder Systemaktivitäten
- Saubere Remediation
  - Passwörter zurücksetzen
    - Umfassendes Zurücksetzen von Passwörtern
    - Für Komplexität bei neuen Passwörtern sorgen
  - Saubere Backups
    - Überprüfen Sie Backups auf potenzielle Bedrohungen
    - Vermeiden Sie die Wiederherstellung von Hintertüren, wie Web-Shells, aus den Backups
- 2-Faktor Authentifizierung

Zusammenfassung

Take-Aways

- **Ransomware-Gruppen werden immer professioneller**
  - Die Methoden gleichen vom Niveau mittlerweile denen von Spionagegruppen
- **Limits von Backups**
  - Sie sind unverzichtbar, aber kein Allheilmittel
    - Angreifer verschlüsseln gezielt Backups
    - Zunahme von Daten-Exfiltration und Erpressung
- **Zukünftige Trends**
  - Gezielte Angriffe auf Cloud-Dienste (Datenspeicher)
  - Nutzung von Grey Zone Devices (Appliances, IOT)
  - Einsatz legitimer Tools (Baselining und Anomalieerkennug)
- **Wiederholte Angriffe**
  - Compromise Assessments nach dem Angriff bringen Klarheit / Sicherheit
- **Ganzheitliches Sicherheitskonzept**
  - Low Hanging Fruits bei Eintrittsvektoren pflücken
  - 80/20 Prinzip anwenden und möglichst viele Disziplinen angehen

The Evolution of Ransomware

From Malware to Sophisticated Cyber Operations

Extra Slides

Microsoft DART Team – most common issues

"This table in the Microsoft Digital Defense Report is always fascinating, these stats are taken from DART engagements and other IR teams, it shows the common issues seen across our customers."

ROM	Issues found	% of customers with the issue
Higher		
15	No advanced MFA protection mechanisms enabled	37%
15	Poor user lifecycle management	21%
15	Lack of EDR coverage	13%
15	Lack of detection controls	10%
13	Resource exposed to public access	2%
12	Insufficient protections for local accounts	60%
12	Missing security barrier between cloud and on-premise	54%
12	Insecure Active Directory configuration	43%
12	Insufficient device security controls	8%
11	Legacy cloud authentication is still used	47%
11	No advanced password protection enabled	37%
11	Missing content based MFA protection mechanisms	24%
11	Insecure operating system configuration	3%
Medium		
8	Legacy and unsecure protocols	18%
7	Missing or inconsistent update management	43%
6	Missing cloud application management and monitoring	21%
6	No privileged identity management solution	8%
6	No MFA, or MFA not mandatory for privileged accounts	21%
6	Weak email protection against common threats	16%
6	Legacy or unsupported operating systems	14%
Lower		
4	No privilege separation	41%
4	No hardened workstations used for administration	23%
4	Missing data classification and sharing restrictions	5%
3	No vulnerability management	30%
2	No adherence to the Least Privilege Principle	63%