

Das kleine 1x1 wie und warum ein Unternehmen gehackt wird

TEMS SECURITY SERVICES



Work smarter
Not harder



Wie sehen wir den IT-Security Wilden Westen

2019 | 2023 (IN 19 TAGEN)

DEADWOOD, SD USA





Wie kann man dem Hacker zum schnellen Erfolg verhelfen

Sicherung mit dem Domänen Admin einrichten

Lokale Administratorenrechte für alle, die behaupten es zu benötigen.

Ein Tier Modell ist einfach zu aufwendig

Admintätigkeiten vom Arbeitsrechner aus ausführen.

Agenda



- 0 | 1
- Huhn-oder-Ei-Problem des Hackers
- Phishing Methoden
- Cybervorfall 1
- Cybervorfall 2
- Cybervorfall 3
- Cybervorfall 4
- Cybervorfall 5
- Zusammenfassung

0 | 1



- Eine Fehlkonfiguration eines Systems
- Ausnutzen einer Schwachstelle einer Software

- **Woraus besteht eigentlich eine Malware / Schadsoftware?**

- Programmteil: Ausnutzen einer Schwachstelle einer Software
- Programmteil: Ausführen von eigener Malware/Schadcode



```
* akir
Hello
!!! Bl00dy Ransomware Gang is Back !!!
!!! Either You Pay Us OR Get Your Company Files/documents Leaked Online For Free !!!
Write to our email ; name your price
decrypt.support@privyonline.com
All computers is hacked and infected with ransomware virus.
*All files/documents/software with '.DRTTY' extension is encrypted*
This means All your computer files,databases,browsers,backups softwares and more
are encrypted . and it is not usable / you cannot open.
ALL Nas, Vcenter, Exsi servers are encrypted
This means you cannot use the files on computers anymore.
1. All encrypted files can only be used or get back to original form
only if you pay for the decryptor software from us , to get all your files back.
*There is no public decryption software. Only our team can help*
We take the money only through Bitcoin and Other crypto.
2. How to contact our team through tox chat
Download tox chat from
https://tox.chat/download.html
send us friend request to tox chat id
E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F
Our team is waiting
>>>> NOTE !!!
4. We are not affiliated or related to any religion, government or entity
Just kindly PAY the ransom and get Decryption software immediately
After payment received we will send private key and decryption software to your IT department !!
!
Free decryption As a guarantee you can send us up to 3 free decrypted files before payment
!!! We have downloaded all your files to our servers and will release data if you do not comply
!!!
!!!Do not attempt to decrypt your data using third-party software this will result in permanent
data loss !!!
```

Ln 8: 33

Hacking 1x1



Hacking 1x1

1. Cyber Kill Chain

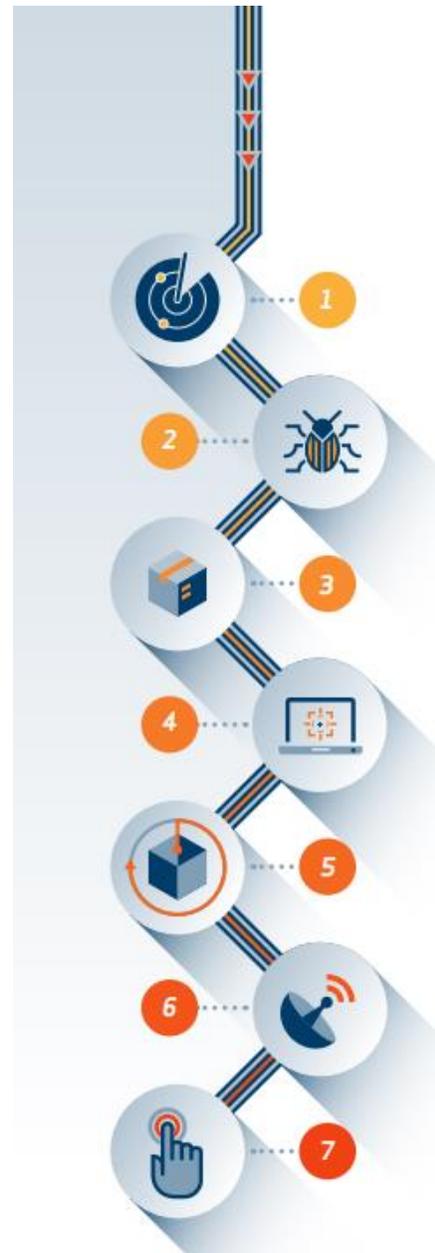


Hacking workflow

WEAPONIZATION

EXPLOITATION

COMMAND & CONTROL (C2)



RECONNAISSANCE

DELIVERY

INSTALLATION

ACTIONS ON OBJECTIVES (*what`s next?*)

MITRE ATT&CK Framework

RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 8 techniques	INITIAL ACCESS 9 techniques	EXECUTION 14 techniques	PERSISTENCE 13 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 42 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 31 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMAND AND CONTROL 16 techniques	EXFILTRATION 9 techniques	IMPACT 13 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Scheduled Task/Job	Valid Accounts	Modify Authentication Process	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction		
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation	Hijack Execution Flow	OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact		
Gather Victim Identity Information	Compromise Infrastructure	Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Direct Volume Access	Input Capture	Replication Through Removable Media	Data Staged	Application Layer Protocol	Data Transfer Size Limits	Service Stop		
Gather Victim Network Information	Establish Accounts	Supply Chain Compromise	Shared Modules	Create or Modify System Process	Rootkit	Brute Force	Internal Spearphishing	Email Collection	Communication Through Removable Media	Exfiltration Over C2 Channel	Inhibit System Recovery		
Gather Victim Ongoing Information	Obtain Capabilities	Hardware Additions	User Execution	Event Triggered Execution	Obfuscated Files or Information	Two-Factor Authentication Interception	Use Alternate Authentication Material	Screen Capture	Exfiltration Over Physical Medium	Defacement			
Phishing for Information	Develop Capabilities	Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution	Process Injection	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer	Multi-Stage Channels	Exfiltration Over Web Service	Firmware Corruption		
Search Closed Sources	Acquire Access	Phishing	System Services	Account Manipulation	Access Token Manipulation	Steal Web Session Cookie	Permission Groups Discovery	Taint Shared Content	Ingress Tool Transfer	Automated Exfiltration	Resource Hijacking		
Search Open Technical Databases	External Remote Services	Command and Scripting Interpreter	External Remote Services	Office Application Startup	Abuse Elevation Control Mechanism	Unsecured Credentials	File and Directory Discovery	Exploitation of Remote Services	Audio Capture	Data Encoding	Endpoint Denial of Service		
Search Open Websites/Domains	Drive-by Compromise	Native API	Native API	Create Account	Domain Policy Modification	Credentials from Password Stores	Peripheral Device Discovery	Remote Service Session Hijacking	Video Capture	Traffic Signaling	System Shutdowns/Reboot		
Search Victim-Owned Websites	Browser Extensions	Inter-Process Communication	Inter-Process Communication	Browser Extensions	Escape to Host	Indicator Removal on Host	Network Share Discovery	Browser Session Hijacking	Browser Session Hijacking	Remote Access Software	Transfer Data to Cloud Account		
	Traffic Signaling	Container Administration Command	Container Administration Command	Traffic Signaling	Exploitation for Privilege Escalation	Modify Registry	Password Policy Discovery	Data from Information Repositories	Data from Information Repositories	Dynamic Resolution	Account Access Removal		
	BITS Jobs	Deploy Container	Deploy Container	BITS Jobs	Server Software Component	Trusted Developer Utilities Proxy Execution	Browser Information Discovery	Data from Network Shared Drive	Adversary-in-the-Middle	Non-Standard Port	Disk Wipe		
	Serverless Execution	Serverless Execution	Serverless Execution	Server Software Component	Pre-OS Boot	Traffic Signaling	Virtualization/Sandbox Evasion	Data from Cloud Storage Object	Signed Script Proxy Execution	Encrypted Channel	Data Manipulation		
	Cloud Administration Command	Cloud Administration Command	Cloud Administration Command	Pre-OS Boot	Compromise Client Software Binary	Rogue Domain Controller	Virtualization/Sandbox Evasion		Adversary-in-the-Middle	Non-Application Layer Protocol			
				Implant Internal Image	Modify Authentication Process	Indirect Command Execution	Cloud Service Dashboard		Forge Web Credentials				
				Modify Authentication Process		BITS Jobs	Software Discovery		Multi-Factor Authentication Request Generation				
						XSL Script Processing	Query Registry		Steal or Forge Authentication Certificates				
						Template Injection	Remote System Discovery						
						File and Directory Permissions Modification	Network Service Scanning						
						Virtualization/Sandbox Evasion	Process Discovery						
						Unused/Unsupported Cloud Regions	System Information Discovery						
						Use Alternate Authentication Material	Account Discovery						
						Impair Defenses	System Time Discovery						
						Hide Artifacts	Domain Trust Discovery						
						Masquerading	Cloud Service Discovery						
						Deobfuscate/Decode Files or Information	Container and Resource Discovery						
						Signed Binary Proxy Execution	Cloud Infrastructure Discovery						
						Exploitation for Defense Evasion	System Location Discovery						
						Execution Guardrails	Cloud Storage Object Discovery						
						Modify Cloud Compute Infrastructure	Group Policy Discovery						
						Pre-OS Boot	Debugger Evasion						
						Subvert Trust Controls	Device Driver Discovery						
						Build Image on Host							
						Deploy Container							
						Modify System Image							
						Network Boundary Bridging							
						Weaken Encryption							
						Reflective Code Loading							
						Debugger Evasion							

Has sub-techniques

MITRE | ATT&CK[®]
Enterprise Framework

attack.mitre.org

Hacking 1x1

2. Wie finde ich verwundbare Systeme?



Huhn oder Ei

<https://crt.sh/>

<https://dnsdumpster.com/>

<https://www.shodan.io/>

<https://www.exploit-db.com/>

<https://www.cvedetails.com/vulnerability-list/>



Passwörter



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Fall 1



Fall 1

7 von 12

- Großes Unternehmen
- Über 5000 Mitarbeiter
- Auf 3 Kontinenten
- 14 Tage ohne IT (weltweit)
- 60 Tage keine E-Mails
- >270 Tage bis Normalbetrieb
- Zentrales Backup zerstört
- Fileserver verschlüsselt
- E-Mail Server verschlüsselt
- Alle Business Applikationen verschlüsselt
- IT war schon immer schlecht
- Mit allen Kosten, die über Jahre eingespart wurden, hatte man externe Consultant gefüttert
- Keine wesentliche Verbesserung nach dem Hackangriff

Fall 2



Fall 2

5 von 12

- Großes Unternehmen
- Über 1000 Mitarbeiter
- Europa
- >10 Tage ohne IT
- >20 Tage keine E-Mails
- >60 Tage bis Normalbetrieb
- Teilweise das Backup zerstört
- Fileserver verschlüsselt
- E-Mail Server verschlüsselt
- Viele Business Applikationen verschlüsselt
- Gute und solide IT
- Eine IT-Hausaufgabe nicht vollständig ausgeführt.
- Hat aus dem Vorfall gelernt

Fall 3



Fall 3

4 von 12

- kleines Unternehmen
- 15 Mitarbeiter
- Österreich
- >2 Tage ohne IT
- >2 Tage keine E-Mails
- 4 Tage bis Normalbetrieb
- Backup war nicht betroffen
- Fileserver verschlüsselt
- Keine E-Mails verschlüsselt
- Keine Business Applikationen verschlüsselt
- Gute und solide IT
- Remote Desktop war nach außen offen.
- Hat aus dem Vorfall gelernt

Fall 4



Fall 4

4 von 12

- kleines Unternehmen
- 7 Mitarbeiter
- Österreich
- >10 Tage ohne IT
- >10 Tage keine E-Mails
- >20 Tage bis Normalbetrieb
- Alles auf einem Server
- Alle E-Mails verschlüsselt
- Server vermietet für Hackangriffe
- Anschließend einfach verschlüsselt
- Hat aus dem Vorfall gelernt

Fall 5



Fall 5 - Sommer 2023

65.000 Mitarbeiter

Die Lockbit-Cybergang ist eine der umtriebigensten kriminellen Vereinigungen. Ende Juni hat die Gruppierung etwa nach einem Einbruch bei einem TSMC-Zulieferer 70 Millionen US-Dollar Lösegeld vom Chipfertiger gefordert. Mitte März

Amount

NT\$1,587,420,000,000

From

 TWD - Taiw

1,587,420,000,000.00 Taiwan New Dollars =

49,657,935,198.16 US Dollars

Amount

NT\$596,540,000,000.00

From

 TWD - Taiw

596,540,000,000.00 Taiwan New Dollars =

18,662,453,357.27 US Dollars

Zu dem Zeitpunkt ging das Unternehmen davon aus, dass die Sicherheitssoftware auch den Abfluss von Daten verhindert hätte. Dem Unternehmen sei noch unklar, welche Informationen genau kopiert wurden, möglicherweise lediglich Daten von dem verwundbaren PC. Es bestehe jedoch das Risiko, dass Daten vom Server kopiert wurden. Das Unternehmen glaube, dass rund 10 Gigabyte an Daten kopiert wurden, was weniger als ein Prozent der gespeicherten Daten sei.

Zusammenfassung





Die Herausforderung für die Hacker

Sicheres Backup

Keine lokalen
Administratoren

Umsetzung
Tier-Level-Modell

Spezielle Admin-
Workstation für
Admins

Aktives Client-Patch
Management

Kein Internetzugriff
für Server

Systemhärtungen
durchführen

Ausnahmslose
MFA Umsetzung

Passwörteränderungen
auch von
Systemkonten

Windows Rechner PW
Änderung alle 3 Tage

Erweitertes Logging in
Windows aktivieren

Installation von
smarten Honeybots



Nützliche Hilfe mit PDF-Dokumenten



- Bei unbedenklichen PDF-Dokumenten
 - <https://www.virustotal.com>
- Online PDF-Viewer
 - <https://smallpdf.com/pdf-reader>
- Online PDF-Analyse
 - <https://pdfux.com/inspect-pdf/>

Aber Vorsicht, sobald Sie ein PDF-Dokument hochgeladen haben, ist es im Internet veröffentlicht.

Vorsicht bei “vermeintlich” vertraulichen PDF-Dokumenten

Einfache IT-Security Spielregeln



- Der Hacker **benötigt nur eine Schwachstelle** oder Fehlkonfiguration, und der Hacker hat Zugriff auf ein Unternehmensnetzwerk.
- Ein Unternehmen kann den Hacker **nur durch Befehl oder falsche Anmeldung** innerhalb des Netzwerks durchführen, und wir sind in der Lage, den Hacker zu erkennen.

Fortbildung und Wissensaufbau sind Schlüsselfaktoren für den Erfolg.

Know
your
limit

Work smarter
Not harder



Source: Internet

Ihr Weg zu einem Expertenteam

<https://tems-security.at>

<https://tems.at>



IT-SECURITY

CYBER-SECURITY

IT-FORENSIC

ONLINE-TERMINBUCHUNG



Buchen Sie **JETZT** Ihren Termin Online

– Die ersten 30 Minuten sind kostenlos –



Philip Berger

IT-Security Specialist, Endpoint Specialist

[Hier gehts zur BUCHUNG »](#)



Michael Meixner, CISSP

DFIR, Incident Response Manager, Forensik Experte

[Hier gehts zur BUCHUNG »](#)



Ing. Alexander Kuchelbacher

IT-Security Specialist, Datacenter Specialist

[Hier gehts zur BUCHUNG »](#)

Buchung EXKLUSIV für Kunden »



Get in contact with us

Philip Berger
Managing Director

 +43(664) 343 8644

 Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

 +43(664) 1453328

 Michael.meixner@tems-security.at