



REDOPS
INFORMATION SECURITY

Cyber Kill Chain

Deep Dive

Whoami

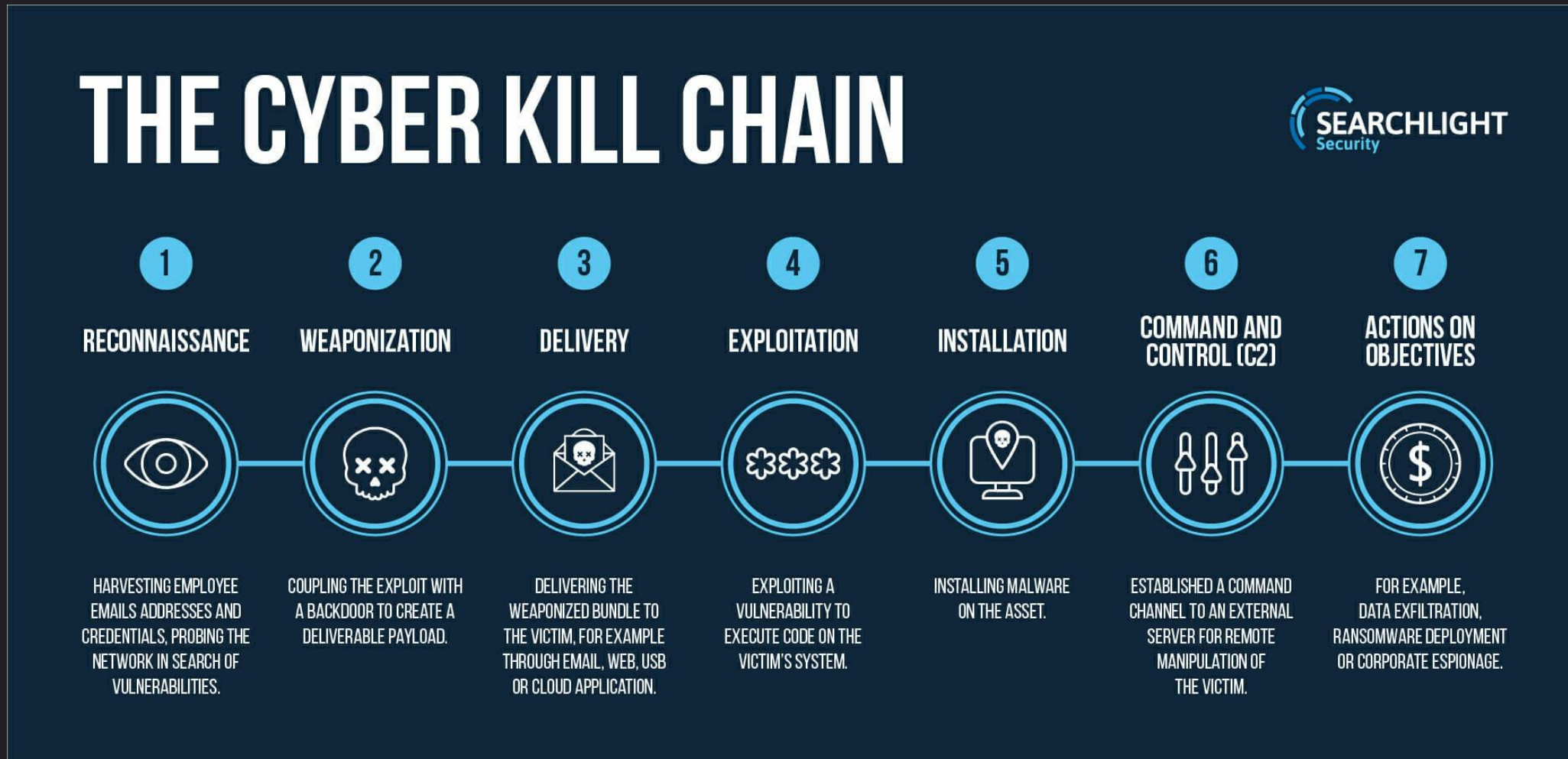
Daniel Feichter Tirol / Thaur

- 12 Jahre Elektronik und Kommunikationstechnik
- Studium Wirtschaftsingenieurwesen
- 5 Jahre in Infosec
- IT-Sec Researcher / [@VirtualAllocEx](https://twitter.com/VirtualAllocEx)
- Gründer RedOps GmbH (vormals Infosec Tirol)
- Mitre Att&ck Contributor (T1562.010, T1562.001)
- Konferenzen: DeepSec, BSides, DEF CON, SANS etc.

Fokus Offensive Security:

- Research: Windows Internals, EDRs, Malware etc.
- Trainings/Workshops, EDR-Evaluation, APT-Simulation etc.
- Red Teaming (SME)

Cyber Kill Chain




Quelle: <https://www.slcyber.io/shifting-left-in-the-cyber-kill-chain/>

Agenda

- Deep Dive Cyber Kill Chain
 - Phase 1 bis Phase 7
- (Live) Demo **EDR Evasion** – Kompromittierung via C2
- Limitierungen Cyber Kill Chain

Blackcat Ransomware

- Praktisches Beispiel -> **Blackcat** Land Kärnten 
- Key Facts Blackcat bzw. ALPHV
 - Ransomware as a Service (Raas)
 - Erstsichtung November 2021
 - Rust
 - Eintrittspunkte:
 - Exchange Server, Kompromittierte Zugangsdaten, Phishing Mail

Phase I

**Reconnaissance /
Taktische Informationsbeschaffung**



Phase I: Reconnaissance

- Red Teaming -> Taktische Informationsbeschaffung
- Möglichst viel relevante Information
- Gute Vorbereitung = Halbe Miete!
- Zeitkontingent Böartiger Hacker vs. Red Team

Aktiv vs. Passiv



- **Passiv:** Öffentlich zugängliche Informationen
- Keine direkte Interaktion mit Ziel
- **I hab nur geschaut!** -> gesetzlich konform



- **Aktiv:** Wir testen was geht
- Direkte Interaktion mit Ziel
- Illegal ohne Permission to Attack

Phase I: Reconnaissance

- Mitarbeiternamen
- E-Mail-Adressen
- Passwörter / Data Breaches
- Software z.B. Betriebssystem, Browser, AV/EPP/EDR etc.
- Sicherheitsprodukte z.B. Firewall, Proxy etc.
- Mögliche Eintrittspunkte

Phase I: Reconnaissance

- Erreichbare Systeme Internet (Schatten-IT)
 - Weitere Informationsbeschaffung
 - Direkte Kompromittierung via Schwachstellen
 - Login Möglichkeiten (HTTP-Formulare, FTP, SSH etc.)

- Freie Domains -> potentiellen Phishing Angriff

Phase I: Reconnaissance

- Tochterunternehmen und Beteiligungen
- Technische Dienstleister
 - Hardware, Software und Infrastruktur
- (Unabsichtlich) geleakte Informationen z.B. Source Code
 - Reddit
 - Stackoverflow, GitHub

Passiv: E-Mail-Adressen



Domain Search ?

🌐 ktn.gv.at 🔍

All Personal Generic 526 results [Export in CSV](#)

Most common pattern: {first}.{last}@ktn.gv.at

Management (5) Support (3) Executive (1) ...

WordPress Content Management System 🔍 + 📧 20+ sources ▾

...@ktn.gv.at ● ✓

Passiv: Data Breaches

';--have i been pwned?

Check if your email or phone is in a data breach

@ktn.gv.at

🔍 pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes ([subscribe](#) to search sensitive breaches)

Passiv: Geleakte Passwörter



domain:ktn.gv.at

1306 RESULT(S) FOUND	134MS SEARCH ELAPSED TIME	14,453,524,343 ASSETS SEARCHED	48,796 AGGREGATED DATA WELLS
-------------------------	------------------------------	-----------------------------------	---------------------------------

Result # 1117891225

Email [redacted]@ktn.gv.at

Password 4c6 [redacted]

Result # 1117891226

Email [redacted]@ktn.gv.at

Password aut [redacted]

Result # 1117891227

Email [redacted]@ktn.gv.at

Password Oks [redacted]

Result # 5804128

Email [redacted]@ktn.gv.at

Password Me [redacted]

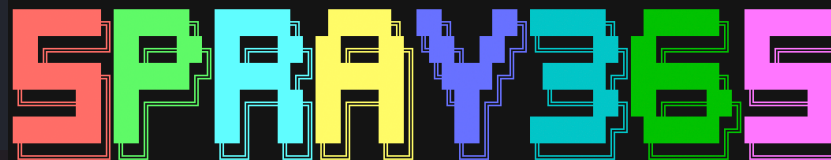
Passiv: Eintrittspunkte

Microsoft 365 supports federated identity. This means that instead of performing the validation of credentials itself, Microsoft 365 refers the connecting user to a federated authentication server that Microsoft 365 trusts. 26.04.2022

```
-# python3 o365chk.py -d ktn.gv.at
```

```
This domain is federated
{
  "AuthURL": "https://adfs.ktn.gv.at/adfs/ls/?username=username%40ktn.gv.at",
  "CloudInstanceIssuerUri": "urn:federation:MicrosoftOnline",
  "CloudInstanceName": "microsoftonline.com",
  "DomainName": "ktn.gv.at",
  "FederationBrandName": "Amt der K\u00e4rntner Landesregierung",
  "FederationGlobalVersion": -1,
  "Login": "username@ktn.gv.at",
  "NameSpaceType": "Federated",
  "State": 3,
  "UserState": 2
}
```

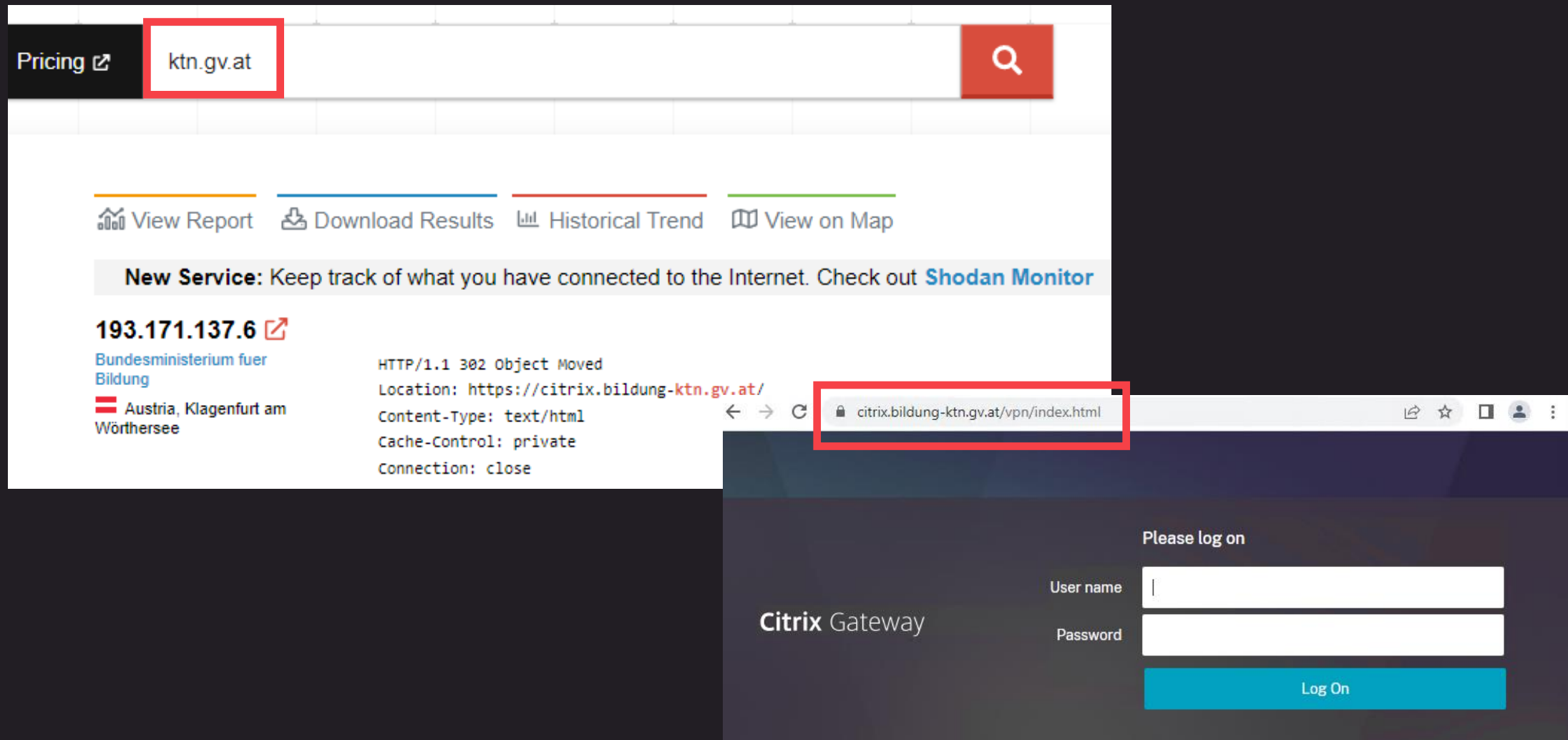
```
> python3 spray365.py -s demo_excpln.json --lockout 10
```



By MarkoH17 (<https://github.com/MarkoH17>)
Version: 0.1.2-beta

```
[2021-12-06 19:46:39 - INFO]: Processing execution plan 'demo_excpln.json'
[2021-12-06 19:46:39 - INFO]: Identified 56 credentials in the provided execution plan
[2021-12-06 19:46:39 - INFO]: Password spraying will take at least 11466 seconds, and sh
[2021-12-06 19:46:39 - INFO]: Lockout threshold is set to 10 accounts
[2021-12-06 19:46:39 - INFO]: Starting to spray credentials
[2021-12-06 19:46:40 - SPRAY 01/56] (win_ie11_win10->o365spo->msmamservice): gwashington
[2021-12-06 19:46:56 - SPRAY 02/56] (win_edge_win10->intune_mam->office_mgmt): mvanburen
```

Passiv: Eintrittspunkte



The screenshot shows a network monitoring tool interface. At the top, there is a search bar with the text "ktn.gv.at" highlighted in a red box. To the left of the search bar is a "Pricing" link with an external icon. Below the search bar, there are four action buttons: "View Report", "Download Results", "Historical Trend", and "View on Map". A notification banner reads: "New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)".

The main content area displays the IP address "193.171.137.6" with an external icon. Below it, the organization name "Bundesministerium fuer Bildung" is shown, followed by a location: "Austria, Klagenfurt am Wörthersee". To the right of this information, the HTTP status "HTTP/1.1 302 Object Moved" is displayed, along with the location "https://citrix.bildung-ktn.gv.at/" and other headers: "Content-Type: text/html", "Cache-Control: private", and "Connection: close".

Below the main content, a browser window is shown. The address bar contains the URL "citrix.bildung-ktn.gv.at/vpn/index.html", which is highlighted in a red box. The browser page displays the "Citrix Gateway" login interface. It features the text "Please log on" and two input fields: "User name" and "Password". A blue "Log On" button is positioned below the password field.



Phase II

Weaponization



Malware: Typen / Familien

Types of Malware

It is short for malicious software which can be used to manipulate your computer and steal your information.



Spyware

Collects information about users without their knowledge.



Ransomware

It blocks the PC, takes control, encrypt your files, and demands a ransom to return them to you.



Adware

Automatically displays or downloads advertising material such as banners or pop-ups when a user is online.



Virus

Damages your data and files via downloads from the internet.



Trojan Horse

A computer program that seems to be a game but in reality, steals/erases information.



Worm

Takes up space and slows your system by making copies of themselves repeatedly.

POLICY

Malware: Windows File Types



Quelle: <https://sensorstechforum.com/de/popular-windows-file-types-used-malware-2018/>

BlackCat: Malicious Macro

Angriff auf Kärnten: Phishing-Mail war Auslöser, Spuren nach Russland

06.06.2022

Patrick Dax

Die Gruppe BlackCat verschaffte sich über ein Phishing-Mail Zugang zu den IT-Systemen des Landes. Ein Datenklau wird weiter nicht bestätigt.

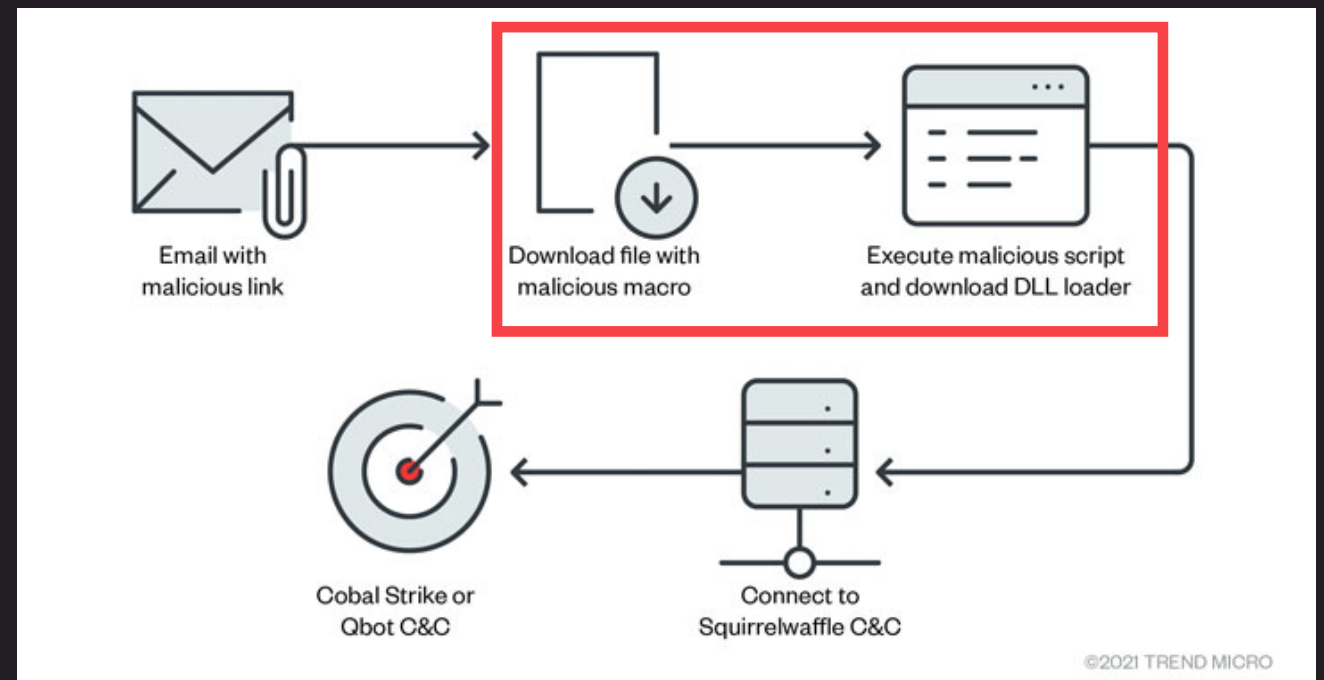
Quelle: <https://futurezone.at/digital-life/cyberangriff-auf-kaernten-phishing-mail-datenleck-blackcat-der/402032804>

Hackerangriff auf Kärnten: Angreifer nutzten Phishing-Mail

08.07.2022

Der Forensikbericht des Cyberangriffs liegt vor. Daran wird bestätigt, dass dessen Ursprung ein Phishing-Mail von April war.

Quelle: <https://futurezone.at/digital-life/hackerangriff-auf-kaernten-cyberattacke-daten-phishing-black-cat/402068170>



Quelle: <https://thehackernews.com/2021/11/hackers-exploiting-proxylogon-and.html>

C2-Malware: Beispiel in C Language

```
int main() {  
    // Insert the Meterpreter shellcode  
    unsigned char code[] = "\xfc\x48\x83...";  
  
    // Allocate Virtual Memory with PAGE_EXECUTE_READWRITE permissions to store the shellcode  
    void* exec = VirtualAlloc(0, sizeof(code), MEM_COMMIT, PAGE_EXECUTE_READWRITE);  
  
    // Copy the shellcode into the allocated memory region using WriteProcessMemory  
    SIZE_T bytesWritten;  
    WriteProcessMemory(GetCurrentProcess(), exec, code, sizeof(code), &bytesWritten);  
  
    // Create a new thread to execute the shellcode  
    HANDLE hThread = CreateThread(NULL, 0, ExecuteShellcode, exec, 0, NULL);  
  
    // Wait for the shellcode execution thread to finish executing  
    WaitForSingleObject(hThread, INFINITE);  
  
    // Return 0 as the main function exit code  
    return 0;  
}
```

GitHub Repo: Workshop

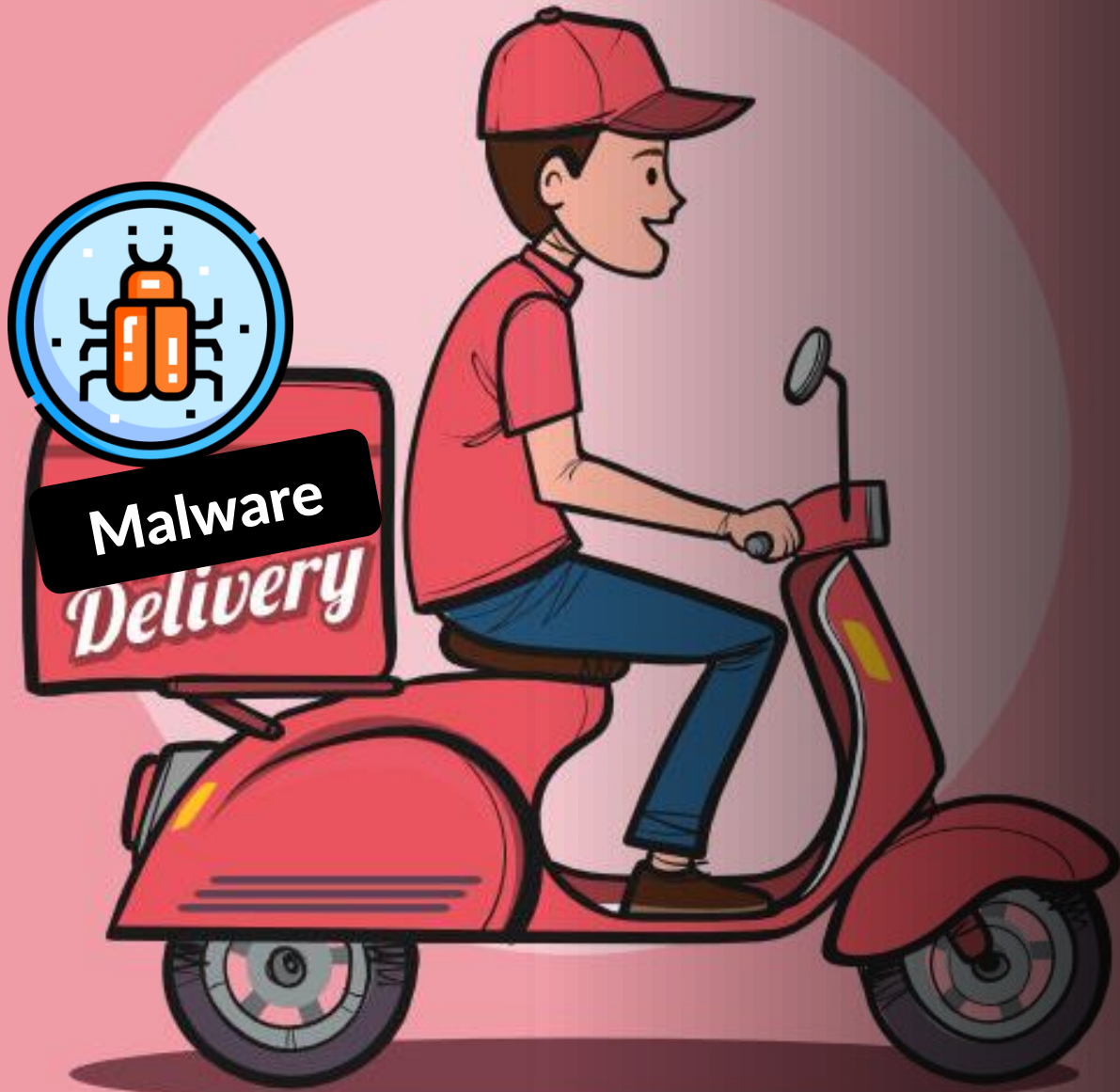
- Check out the following GitHub Repository
- Get Hands on! -> Syscall Workshop

<https://github.com/VirtualAllocEx/DEFCON-31-Syscalls-Workshop>

All the **theory** and **playbooks for the exercises** can be found in the [wiki](#), which together with the prepared POCs is the heart of this project. The **POCs for the exercises** can be found here on the **main page**.

Happy Learning!

Daniel Feichter [@VirtualAllocEx](#), Founder [@RedOps](#) Information Security



Phase III

Delivery



Malware **Delivery**

BlackCat: Initial Access via Phishing

Angriff auf Kärnten: Phishing-Mail war Auslöser, Spuren nach Russland



06.06.2022

Patrick Dax

Die Gruppe BlackCat verschaffte sich über ein Phishing-Mail Zugang zu den IT-Systemen des Landes. Ein Datenklau wird weiter nicht bestätigt.

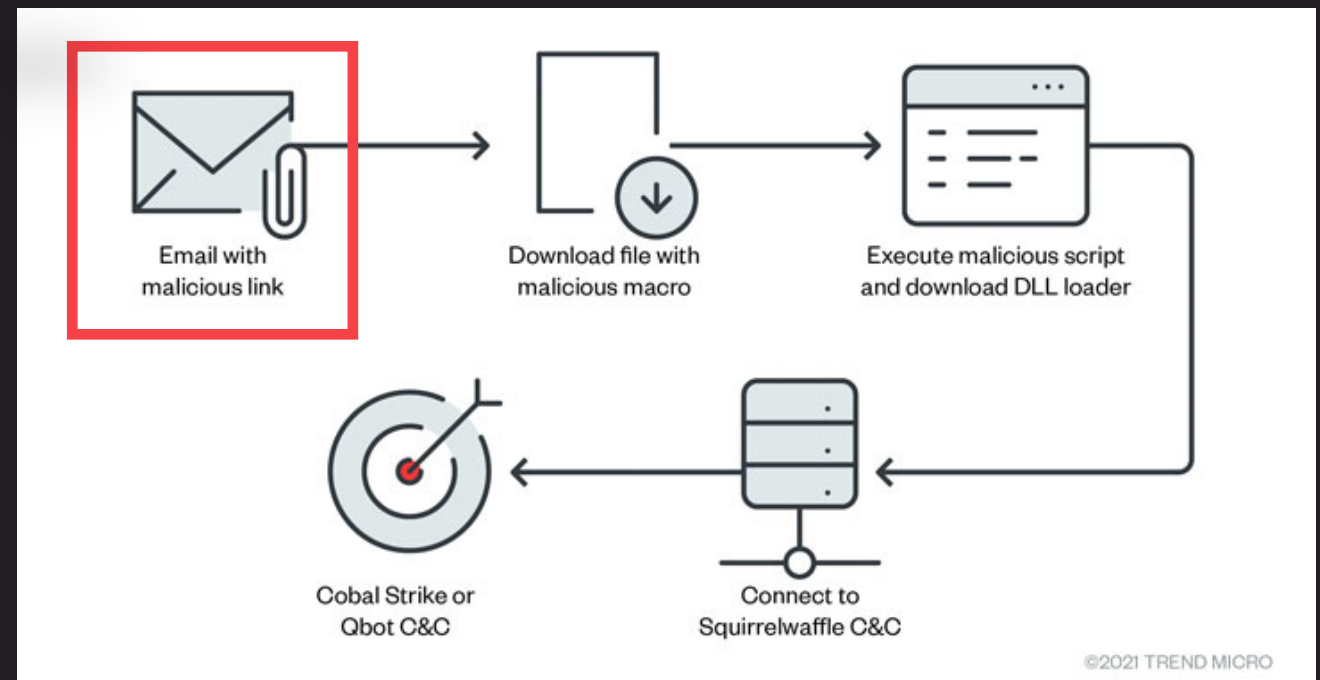
Quelle: <https://futurezone.at/digital-life/cyberangriff-auf-kaernten-phishing-mail-datenleck-blackcat-der/402032804>

Hackerangriff auf Kärnten: Angreifer nutzten Phishing-Mail

08.07.2022

Der Forensikbericht des Cyberangriffs liegt vor. Daran wird bestätigt, dass dessen Ursprung ein Phishing-Mail von April war.

Quelle: <https://futurezone.at/digital-life/hackerangriff-auf-kaernten-cyberattacke-daten-phishing-black-cat/402068170>



Quelle: <https://thehackernews.com/2021/11/hackers-exploiting-proxylogon-and.html>

Phase IV

Exploitation



Phase IV: Exploitation

- Schwachstelle = Vulnerability
- Schwachstelle -> ausnutzen via Exploit -> Exploitation
- ProxyShell, PrintNightmare, Folina etc.
- **Remote Code Execution (RCE)**
- Red Teaming optional bzw. gut abwägen/abstimmen
- **Exploit-DB**

Phase V

Installation



The installation was completed successfully.



The installation was successful.

The malware was installed.

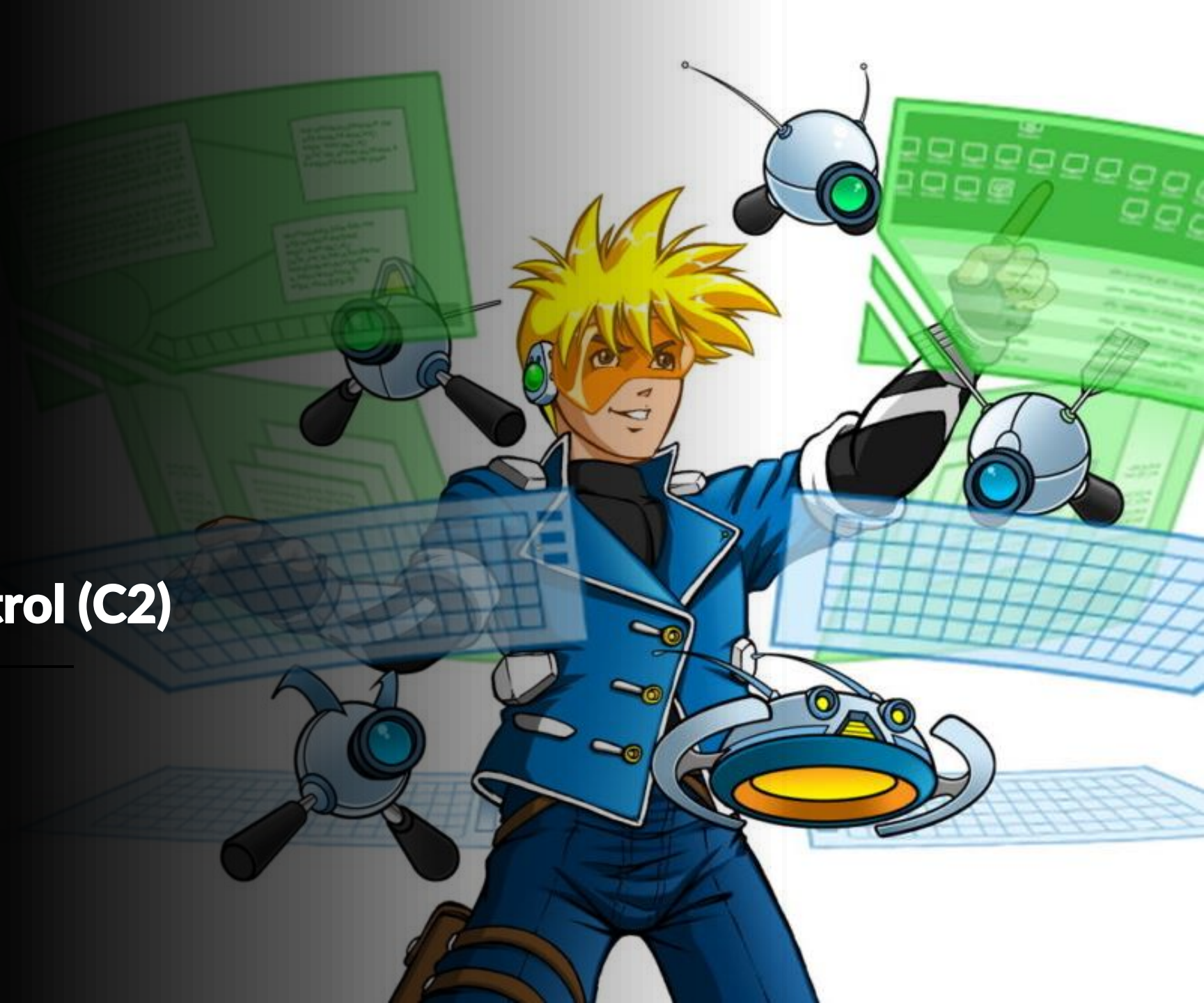
Phase V: Installation

- Rootkit Installation
- Keylogger
- Hidden RDP
- Fallback Channel
- Persistenz: Registry, Scheduled Tasks etc.
- Etc.



Phase VI

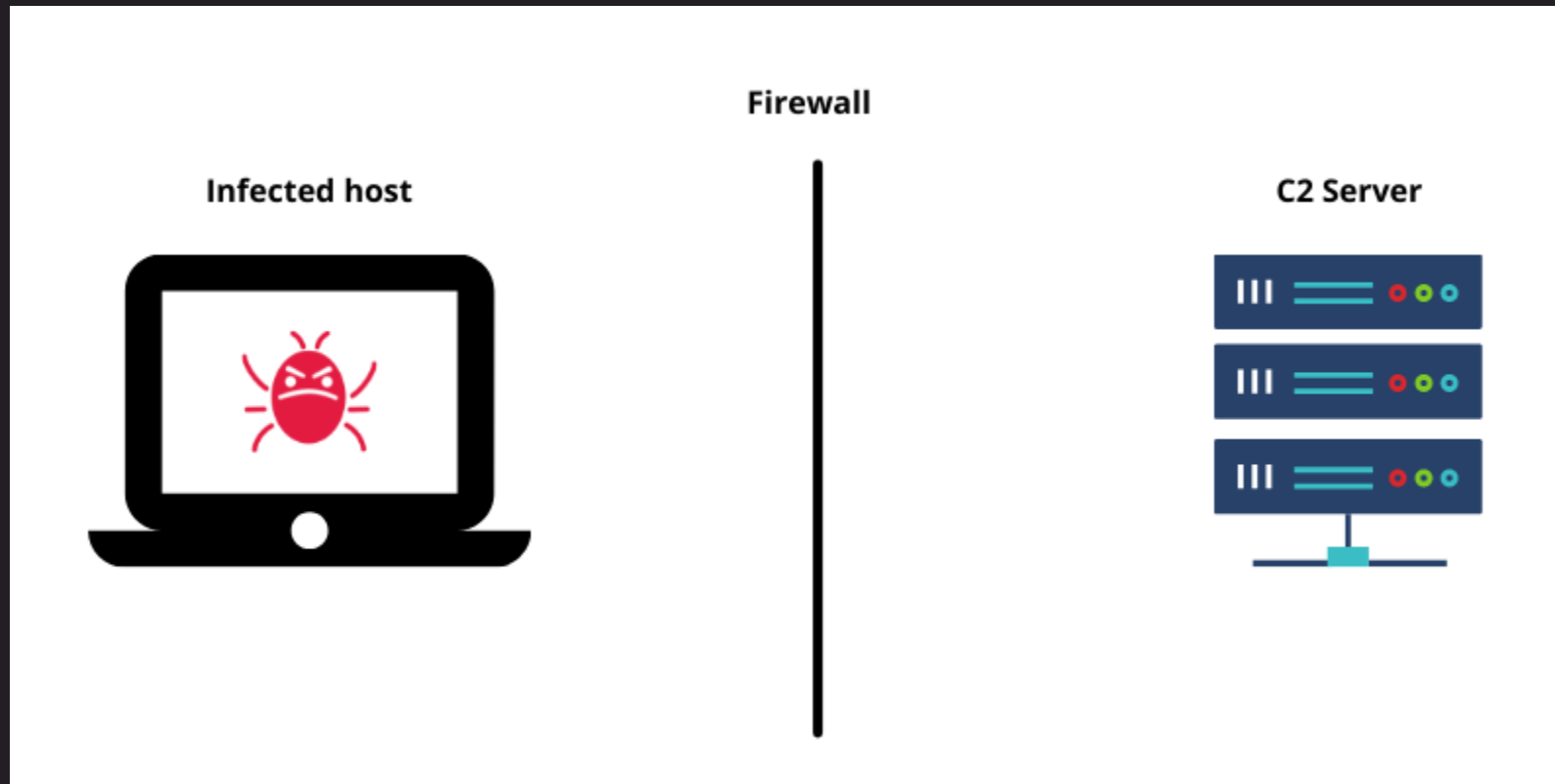
Command and Control (C2)



Phase VI: Command and Control

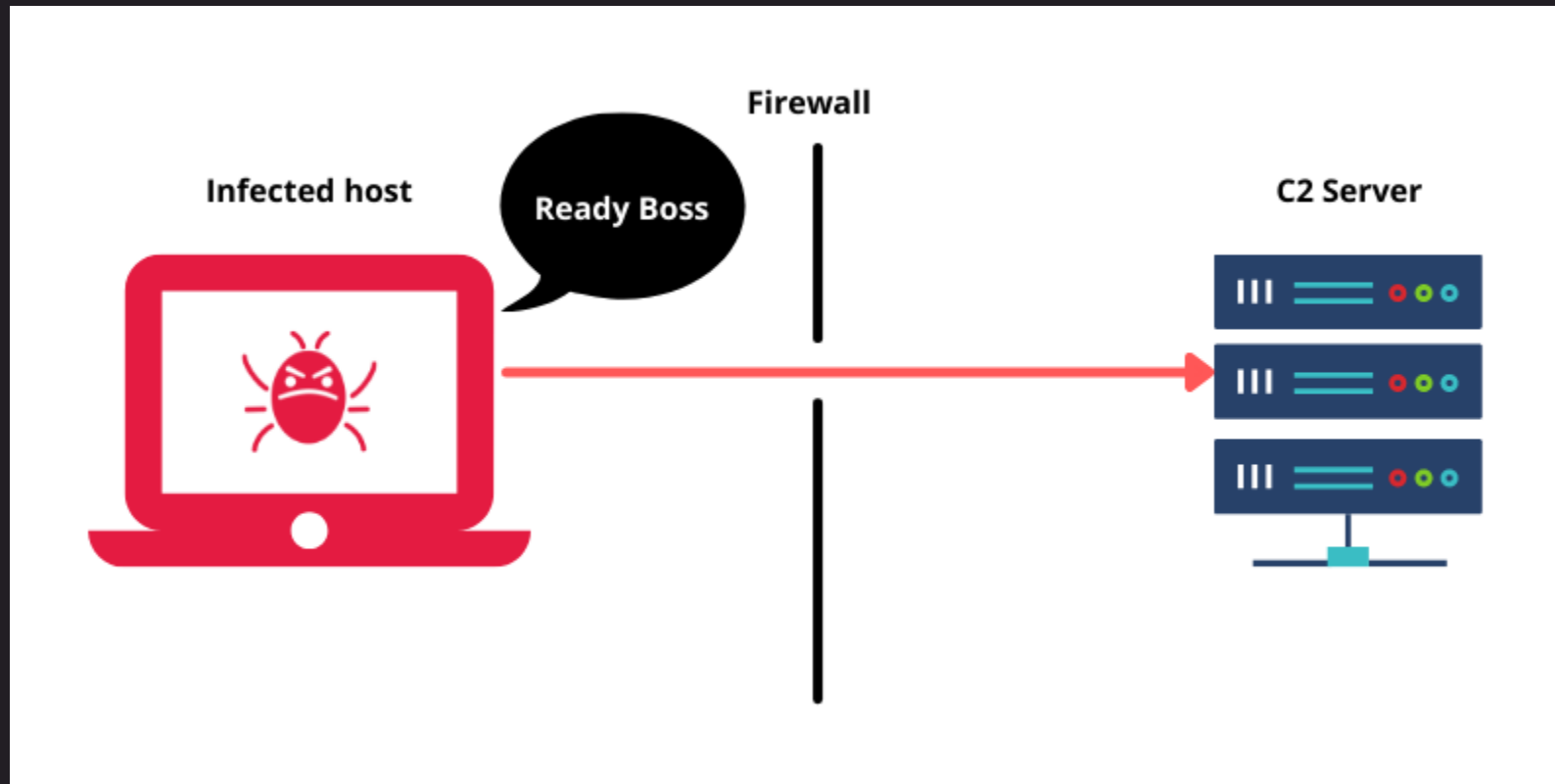
- Malware -> Aufbau C2
- Malware öffnet Kommunikationskanal -> https, http, tcp, dns etc.
 - Beacon
 - Badger
 - Etc.
- Malware Development -> unentdeckt von AV/EPP/EDR/FW etc.

Phase VI: Command and Control



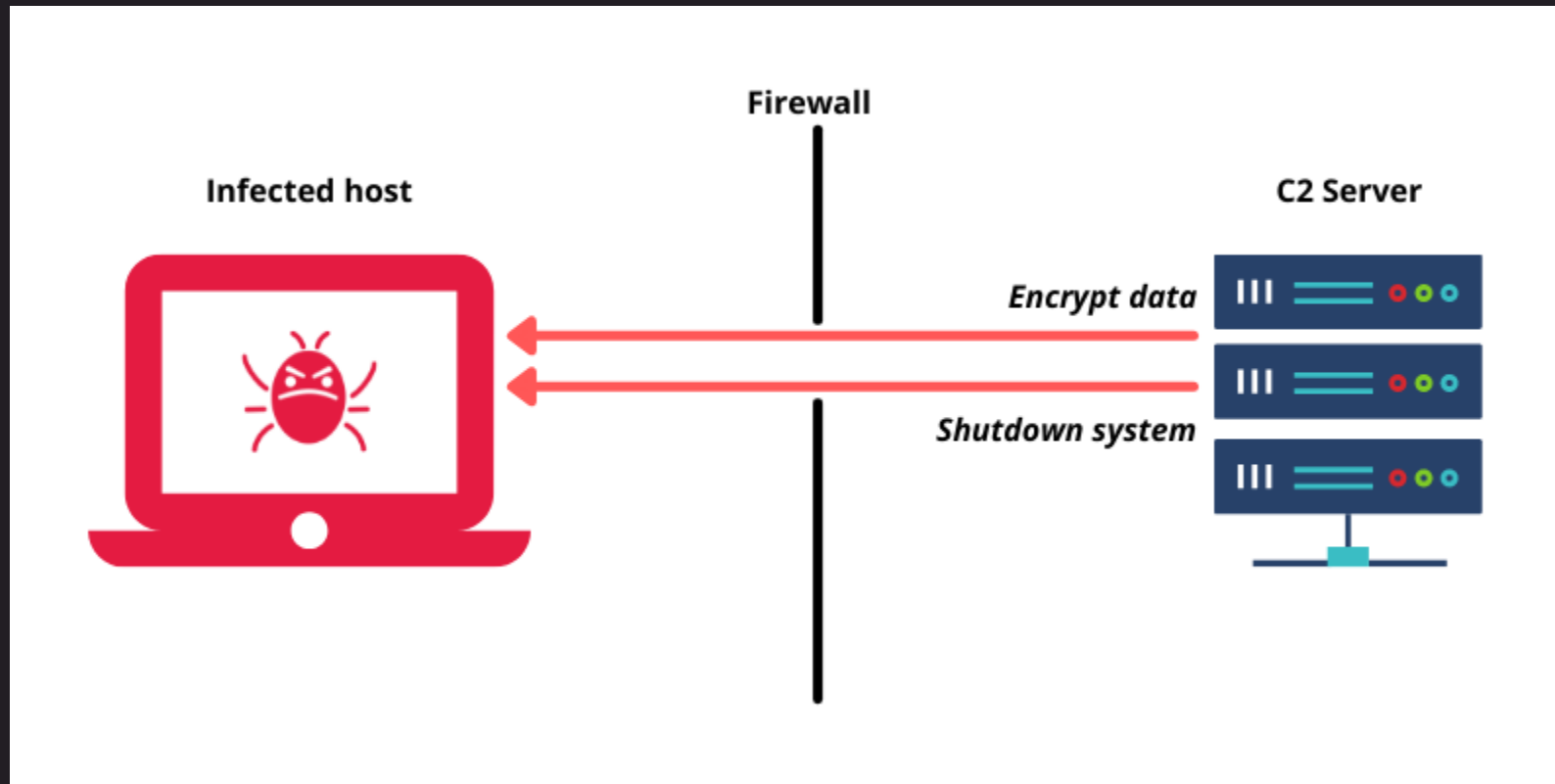
Quelle: <https://www.dnsfilter.com/blog/c2-server-command-and-control-attack>

Phase VI: Command and Control



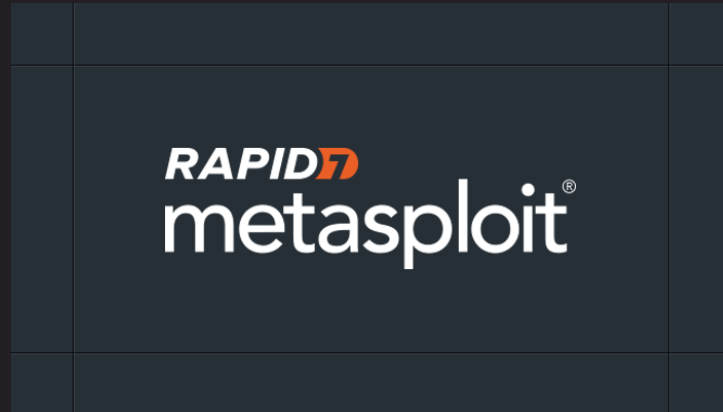
Quelle: <https://www.dnsfilter.com/blog/c2-server-command-and-control-attack>

Phase VI: Command and Control



Quelle: <https://www.dnsfilter.com/blog/c2-server-command-and-control-attack>

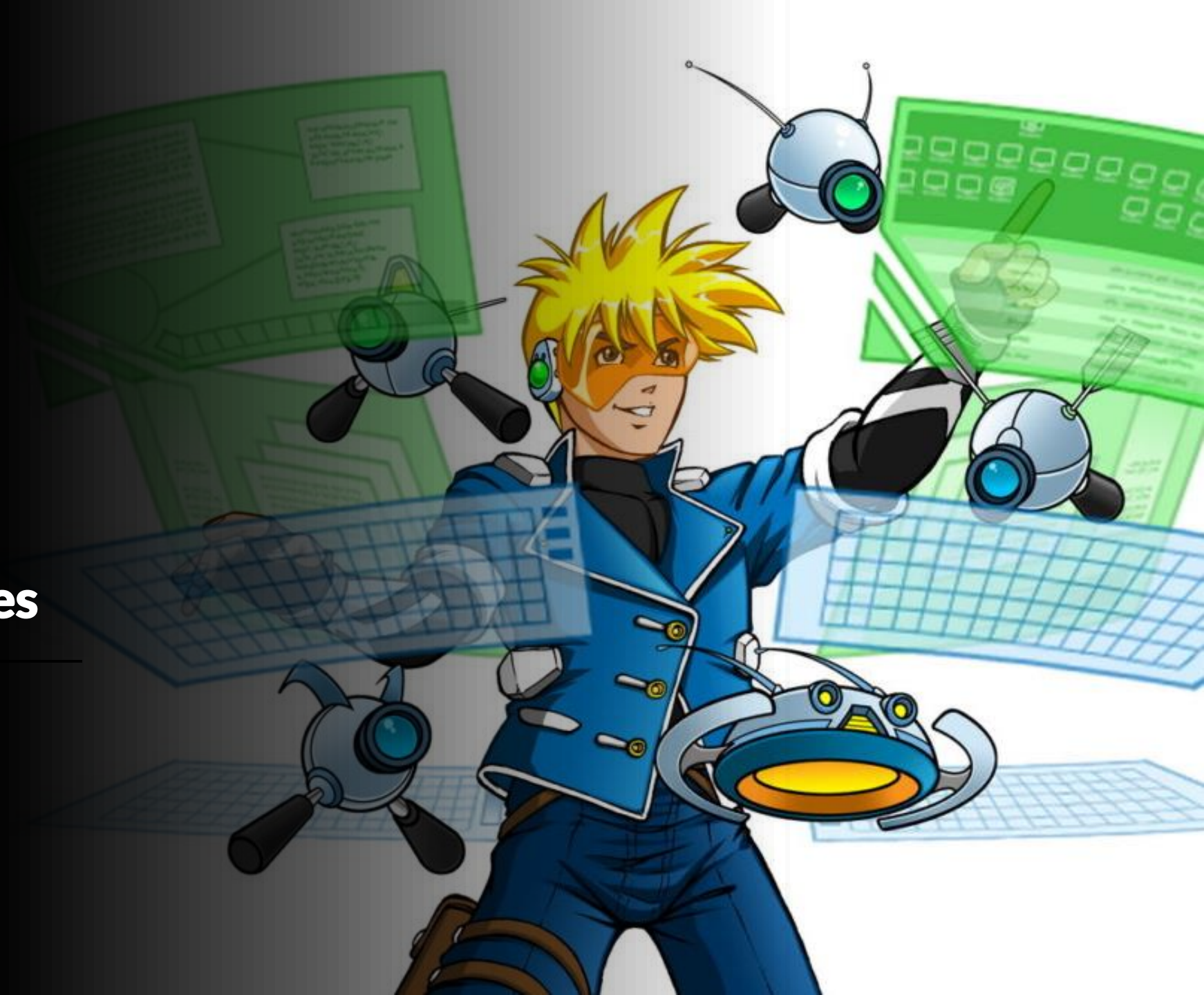
Phase VI: C2 Frameworks





Phase VII

Action on Objectives



Phase VII: Action on Objectives

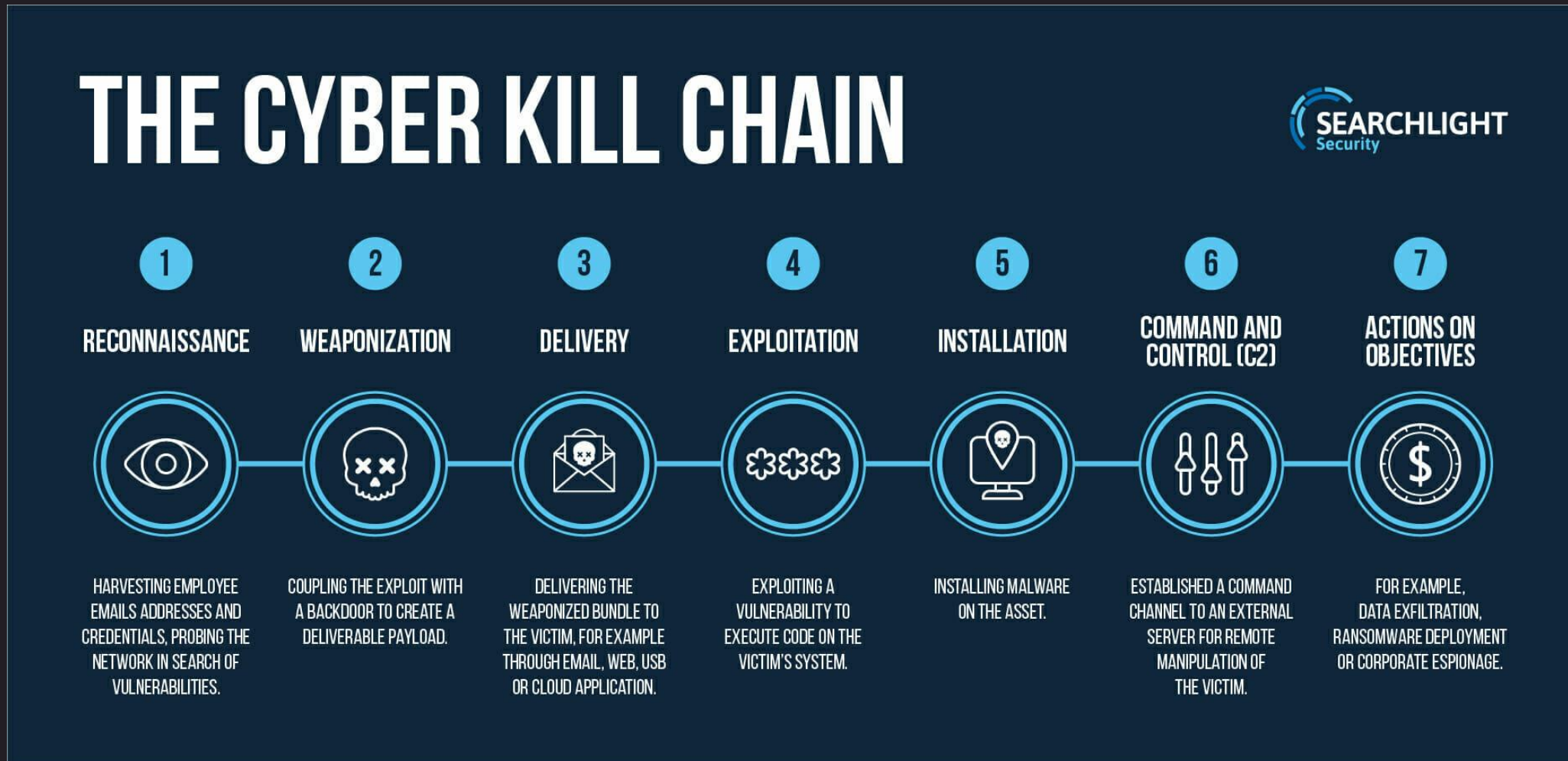
- Spionage
- Manipulation von Daten / Integrität
- Data Exfiltration
- Ransomware / Verschlüsselung von Daten
- Destruction of data
- Etc.

Demo: C2-Initial Access



Quelle: <https://reciprocity.com/resources/what-are-cybersecurity-threats/>

Summary: Cyber Kill Chain



Quelle: <https://www.slcyber.io/shifting-left-in-the-cyber-kill-chain/>

Cyber Kill Chain Limitierungen

- **Lineare Struktur** -> Cyberangriffe oft nicht linear, und Angreifer können Phasen überspringen, kombinieren oder wiederholen.
- Unfähigkeit, interne Bedrohungen und webbasierte Angriffe zu erkennen
- Die sich verändernde Landschaft der Cyber-Bedrohungen

Cyber Kill Chain Limitierungen

- Gute Beschreibung Cyberangriff von Reconnaissance bis Initial Access
- Für spätere Phasen -> Post Exploitation -> Mitre Att&ck Framework

ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Accounts (3)	External		Boot or Logon Autostart Execution (14)	BITS Jobs	BITS Jobs	Credentials from Password	Browser Information Discovery



Vielen Dank! Q & A

- Website: <https://redops.at>
- E-Mail: office@redops.at
- LinkedIn: [Daniel Feichter](#)
- Twitter: [@VirtualAllocEx](#)

Quellen & Referenzen

- <https://futurezone.at/digital-life/cyberangriff-hacker-kaernten-daten-leak-80000-stammdaten-black-cat-ransomware/402037806>
- <https://futurezone.at/digital-life/cyberangriff-medizinische-universitaet-innsbruck/402054436>
- <https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsberichte/2021-BMI-Cybercrime-Report.html>
- https://bundeskriminalamt.at/306/files/2022-222_Cybercrime_Report_2021_-_V20220621_1030_webBF.pdf
- <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>
- <https://www.sungardas.com/en-us/blog/the-consequences-of-a-cyber-security-breach/>
- <https://www.tt.com/artikel/30824225/cyberangriff-auf-innsbrucker-med-uni-daten-im-darknet-veroeffentlicht>
- <https://futurezone.at/netzpolitik/hacker-angriff-kaernten-daten-angeblich-verkauft-blackcat/402061315>
- <https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/>
- <https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f>
- <https://tryhackme.com/room/passiverecon>
- <https://hunter.io/search/ktn.gv.at>
- <http://metricsparrow.com/toolkit/email-permutator/>
- <https://github.com/nixintel/o365chk>

Quellen & Referenzen

- <https://www.shodan.io/search?query=ktn.gv.at>
- <https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/>
- <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>
- <https://thehackernews.com/2021/11/hackers-exploiting-proxylogon-and.html>
- <https://unit42.paloaltonetworks.com/blackcat-ransomware/>
- <https://www.dnsfilter.com/blog/c2-server-command-and-control-attack>
- <https://www.ic3.gov/Media/News/2022/220420.pdf>
- <https://twitter.com/PollicyOrg/status/1260917030393450496>
- <https://www.borncity.com/blog/2022/06/07/cyberangriff-auf-landesregierung-krnten-black-cat-gruppe-verffentlicht-private-daten/>
- <https://www.ic3.gov/Media/News/2022/220420.pdf>
- <https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/>
- <https://futurezone.at/digital-life/hackerangriff-auf-kaernten-cyberattacke-daten-phishing-black-cat/402068170>
- <https://www.ikarussecurity.com/security-news/schutz-vor-blackcat-ransomware/>

Quellen & Referenzen

- <https://www.varonis.com/blog/blackcat-ransomware>
- <https://www.exabeam.com/information-security/cyber-kill-chain/>
- <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
- <https://www.pncpa.com/insights/combating-fraud-search-for-silver-bullet/>
- <https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>
- <https://www.nstec.com/network-security/cybersecurity/what-is-perimeter-defense-in-cybersecurity/>
- <https://reciprocity.com/resources/what-are-cybersecurity-threats/>
- https://redteam.guide/docs/Concepts/mitre_attack/
- <https://blog.smu.edu/itconnect/2021/07/01/printnightmare-windows-security-vulnerability-printing-services/>
- <https://www.hornetsecurity.com/en/knowledge-base/cyber-kill-chain/>
- <https://www.linkedin.com/pulse/mastering-cyber-kill-chain-comprehensive-insight-optimal-utilization/>
- <https://www.slcyber.io/shifting-left-in-the-cyber-kill-chain/>