FontPack: A dangerous update

i blog.group-ib.com/fontpack



03.06.2021

Attribution secrets: Who is behind stealing credentials and bank card data by asking to install fake Flash Player, browser or font updates?

Attribution is our main focus here at Group-IB Threat Intelligence & Attribution, and it becomes harder every year. The number of unique malicious programs is decreasing while affiliate programs (collaborations between threat actors) are on the rise, with the number and quality of attacks both going up. Today **Nikita Rostovtsev**, an analyst at Group-IB Threat Intelligence, will show you attribution in practice by examining a malicious landing page that Group-IB specialists are tracking as FontPack. You will see what this page distributes and how it does so, as well as learn other interesting things that Group-IB has uncovered.

First and foremost we need to find out who is behind the landing page, down to the specific hacking group or particular threat actor. All we know so far is that the page is hosted on compromised websites by injecting JS scripts. The scripts imitate a website crashing and display a message saying that users must update their software, e.g., the browser, Adobe Flash Player, or fonts. The code name used by our team, FontPack, is based on the decoy methods employed in the campaign we will analyze in this report.

Threat actors decide what particular fake to show their victim and how often to do so by changing relevant variables in the script code. According to our data, multiple unconnected hackers use the tool.

Let us focus on one campaign whose goal was to deliver the RedLine stealer to victim devices. When successful, threat actors were able to collect their victims' credentials, autocomplete field data, and bank card information. Our analysis revealed that, since November 2020, FontPack has infected at least 20 websites, including six that were involved in one campaign. But first things first.

What is FontPack?

By "landing page" we mean a target webpage that is shown to users and urges them to download a malicious file that will then be executed. The FontPack landing page has been known to Threat Intelligence & Attribution researchers since 2018. <u>Other specialists</u> may know it as "Domen toolkit" because of its variable called "var domen". How is FontPack injected into websites?

Attacks start with injecting FontPack-containing JS scripts into websites created and controlled by the threat actors. Compromised legitimate websites are also used for the same purpose.

⑦ School Of Film And Telev × +	
← → C 🔏 www.mitsft.in	··· ☆ O ¥. =
THE COLLOCATION OF THE	
Firefox Update Center	mozilla
You are using an older version of the brows In connection with the release of a new version outdated versions:	ser Firefox (56.0). of the browser from 19.04.2021 possible errors in the work of
Tringer Setting Incorrect site mapping	
Loss of all stored and personal data	
Browser errors	
To fix errors and save your data, update your br	rowser to the latest version Update
	National Education Excellence Awards, 2017, by ASSOCHAM. The University is non-affiliating university, situated at Rajbaug Campus, Loni Kalbhor, Pune-Solapur Highway, Pune, India.
Make An Enquiry cick here	The University is self-financed University empowered to award the degrees under section 22 of the University Grants Commission Act 1956

A fake window urging the user to update their browser, shown on top of a legitimate website

Often, victims visit websites that they trust and that they have already been visiting for months, until one day the website asks them to update an outdated plugin. When they do so, malware is downloaded to their computer. This type of attack is the most effective for threat actors and the most dangerous for regular users because victims do not suspect an infection from a website they trust. Readers who do not yet understand what such websites can look like might find the gif below helpful:

So, what exactly happened there? We see that a user goes to a website that they have visited before. After the victim spends some time there, the website contents starts to visually "break" and the browser asks the user to update Flash Player so that everything works properly again. The victim does so.

Landing page code analysis

To understand how such attacks work, we looked at the contents of the malicious JS script. By analyzing the website contents, we detected a JS script called "wp-kernel.js".



Example of FontPack landing page code showing that a fake website created using it will work both on desktop computers and mobile devices

The script contents clearly show that, in addition to personal computers, it can infect mobile devices running Android and Blackberry OS, as well as devices that use the mobile browsers IEMobile and Opera Mini. The script identifies what browser is used for the connection and based on this information provides the victim with a link to the relevant file. The script changes fake windows by changing the value of the variable *var banner*:



In connection with the release of a new version of the browser from **04.10.2018** possible errors in the work of outdated versions:



To fix errors and save your data, update your browser to the latest version

Update

 \times

Fake browser update window



The 'PT Sans' font wasn't found

The web page you are trying to load is displayed incorrectly, as it uses the 'PT Sans' font. To fix the error and display the text, you have to update the 'Chrome Font Pack'.

Manufacturer:	Chrome
Current version:	Font Pack 23.43.5443.12
Latest version:	Font Pack 28.56.5543.23

Fake font update window

	Flash Player Update Recommended
F	Please install the new Flash Player
	 Based on ffmpeg the leading Audio/Video codec library Supports *.FLV, *.AVI, *.MPEG, *.MOW, *.MKV, *.SWF and more Super fast and user-friendly interface 100% Free & Safe
	Updating takes a few seconds and no restart needed after installation.
LATER	UPDATE

Fake Adobe Flash Player update window

The variable var startTime sets the time (in milliseconds) after which the user will be shown a fake window.

The variable var linkMobile creates a link to an app for mobile devices (the link is not active in this particular case). As a result, in this particular campaign, we could only identify an infection designed for the Windows operating system.

As mentioned above, when the script is working website contents are visually distorted — this is what the variable var bugs does. For this to happen, the variable must be set to True. When the variable is set to False, there are no changes to the website.

The variable oneTimeShow, sets the frequency with which the script functions. If the variable is set to True, the script will only function once for every user.

Update

In addition, the script contains a set of 27 language systems for which the fake windows will be shown. Spoiler alert: you will not find anything related to the post-Soviet region there.

The aim of the report is not to describe how the script works in detail, however, so let us move on.

The JS script code has the variable var domen with the value browsertelemetry[.]tk. The domain contains an admin panel hosted at https://browsertelemetry[.]tk/admin/login.

The admin panel uses the Cyrillic alphabet on the authentication page:

Login		×	+	
← → C	A https://b	rowse	rtelemetry.tk/admin/login	
Ĭ				
			Вуол	
			Бход	
			Логин	
			Пародь	
			Пароль	
			Войти	

Admin panel used in the FontPack campaign

Underground platform profile analysis

In a report released on February 28, 2020, Malwarebytes researchers showed that the landing page in question was put up for sale on April 10, 2019. In a screenshot provided by the researchers, the thread author is a user with the username xxbtc. The same landing page was distributed by users with the usernames grinGo and holeo. It is noteworthy that the item was put up for sale by three different users on different underground platforms.



Every screenshot above has roughly the same text (with some variation) about selling a Russian-language landing page with the following content:

"Script for achieving EXE/APK installations!

The script is designed for achieving installations from websites/shells/fakes

It is adapted to both computers and mobile devices

The JS script connects to any website through <script>"

Interestingly, six days later xxbtc invited forum users to test MagBo, an exchange for trading shells. Let us note this fact and return to it later.

Nickname	Source blacktip.top	ß	Topic name	TRANSLATE
Neckname xotte 19 Avatars ∎ 1 Telegram € read xobto@exploit im	Source blacktip top Fran message 18.01.2019	2 Last message 16042019	Торіс палає Мадії обрана доступов Торіс палаєда Порагалає зам поучастворавни бираки улян-гродани шеллов. Так ке инжеста дургої цифоров ї тастировани бираки улян-гродани шеллов. Так ке инжеста дургої цифоров ї тастировани бираки улян-гродани шеллов. 1 ак се инжеста дургої цифоров ї тастировани бираки улян-гродани шеллов. 1 ак се инжеста дургої цифоров ї тастировани бираки улян-гродани шеллов. 1 ак се инжеста дургої цифоров ї тастировани бираки улян-гродани шеллов. 1 ак се инжеста дургої цифоров от силистировани бираки у пала та така и така	TRANGLATE
			В "один руки": один кост - один продавец + один покупатель, но есть возможность "перепрадать" товар теми, кто купил. Возможность сусыравть домак эксто при продавже (не рекомендуется). Возможность мочетназвии доступов.	
			Просода отнестное, о пониманием к возможным проблемых система находится на стадии альфа, но, по понятным причинам, с тестировщиками некоторый дефицит, поэтому тестирован честично отпристрателя Версия, опол присустратера, на пока отключена, что бы тестировать без учетов глокое Тос.	ие
			Риботьют так вс следующие затегории товаров: продаже комплетото сомое документов. Разрабатываются следующие категории товаров: продаже дедиков, продаже мошелькое (с автопререприяваной), продаже аккиритов (соц сети, доски, Adsense). Так не будат работать: сбитсай миноские об ибелием (с продаже аписией от чистых bits ношелькое читов).	

MagBo is slowly entering our story...

The user shared an invite code: CTXDDYMGFJ. According to our data, six users on various platforms posted similar messages with the same invite code.

Xxtbc, xenys, gonleen, amlogic, grinGo, and pacificcc.

In addition, a uniting factor for some of these usernames are Jabber and Telegram mentioned for communication purposes.

xxxbtc@exploit.im and @xengf

Xxbtc, kista, holeo, xenys, amlogic, exynos, gringo, and pacificcc.

15.10.2019 10:57	Cains Jons Buggew exe Translated Websites for issuing exe I fud ws 1 24.05.2019 – 24.04.2021 8, 1 12 11	Acryansko nochjave pas gav ljeva 503 Telegram <mark>(skolo)</mark> oveka Konsulož kommert sa oveka kvalovo ljevy! Translated: Actual last tivo dvja price 50 š Telegram (gjerogi very langa set for a very low price!	
15.10.2019 10:56	Califia Joné augesure en Translated Webdiels for issuing eine Skynetzone pix 🗂 22.05.2019 – 15.10.2019 🔗 1 📧 9	Actyonauo nochquee paa guee 503 Telegram (second) Translated: Actual last two days price 50 3 Telegram @nerof @ webci	
14.10.2019 22:36	Craw, caims pan abugsvu sautero oxel Translated Scam, atter for issuing your exel winh club net C 16.02.2019 – 24.11.2019 R 17 JE 76	Actyonato nochtaine paa gue gens 503 Telegram (axtend) Translated: Actual last two days price 50 3 Telegram (© pandfoce	

The same Telegram account associated with different usernames. "For the last two days of the offer, the price is \$50. Telegram @xengf. A big set for a very low price!"

It is highly likely that the above means that these accounts belong to one person. Below is a mind map we created that makes our conclusion clearer.



Interrelations between different profiles that highly likely belong to one person

How does MagBo factor in?

According to our data, since November 2020 the landing page in question has infected at least 20 websites, including six involved in one campaign, i.e. linked to the domain browsertelemetry[.]tk. It is worth noting that access to some of these websites was sold on MagBo. In addition, posts made by xxxbtc on MagBo included messages about selling logs for November–December 2020.

			LO 2000	G Mb	
Туре:	Не пр	едоставлен системе			
ID:	1114				
6 с лиц Из 800-	иним тысяч логов -1200 логов выде;	з за Ноябрь Декабрь онута крипта - оста/	ньное не тронуто и д 400.00	цаже не чекано Виу	
			Bargain a price dow	n! Bid a fair price!	
seller xxxbto	C ru				
0 ⊠	8 purchases	2 sales	\$17 total	1 review	4.00
Options	5				
Coun	ntry				
Size					2000

Logs sold on MagBo by a user we are already familiar with: xxxbtc. "Over 6,000 logs for November December. 800-1,200 logs had cryptos extracted – the rest hasn't been touched and hasn't even been checked"

So who is the author of the landing page?

A more in-depth analysis revealed that the landing page we call FontPack was put up for sale by a seller with the username DR.PREDATOR in January 2018.

Nickname			Торіс патте	ANSLATE
DR.PREDATOR	exploit.in		Скрипт «Install Pack» для EXEVAPK Инсталов	
Maccanae				
messages	04 00 0017	cust message	http://d.zaix.ru/99gA.png	
1155	24.08.2017	31.07.2020	Кому интересны детали работы лендинга стучите по контактам !	
Avatars			OFINCAHUE\DESCRIPTION :	
			Спойлер	
- <u>-</u>			РУССКИЙ:	
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			Скрипт предназначен для добычи инсталлов с сайтов/шеллов/фейков.	
Telegram			Подходит для добычи инсталлов как с ПК, так и с АПК.	
@evoloit @VIIC07824	ODP DPEDATOR Onwealf		Вы подключаете скрипт к нужному ресурсу и посетителям под разными предлогами (в зависимости от выбранного метода разводки) будет предлагаться скачать и установить файл.	
(pexploit (prodovoza	WDR_PREDATOR (withysen		На двиный момент скрипт включает в себя 3 метода разводки:	
			1. Фейк «Обновление браузера»	
E-mail			Принцип работы:	
Too many contacts!			 Человек заходит на сайт, спустя пару секунд начинается имитация багов и некорректности работы браузера, для того чтобы убедить человека что с браузером что то не так. 	
roo many contacto.			 Далее происходит появление модального окна (non an) в стиле браузера. Модальное окно сообщает о том что человек использует старую версию браузера и из-за этого возможны проблем 	мыи
			бати в работе браузера. И для устранения этих багов необходимо обновить браузер до актуальной версии.	
Phone			3) После нажатия на «Обновить» происходит скачивание фаила.	
- 4			2. Феик «шрифт не наиден» —	
			Принцип расоты:	
			 1) человек заходит на свит и видит что на свите вместо окојчных шрифтов показаны какие то спецсимволы Оправно на свите вместо окојчных шрифтов показаны какие то спецсимволы 	
			2) далее происходит помаление мидального сика (пол ал) и слиле оразера, мидальное ские соорадет о том что у него отсутствует дрифт и из-за этото корректное оторажение саита не возк И ла устальника этой проблемы необходими обновить стальлатный Болг Раск в саком блаумеле.	иожно
			3) После нажатия на «Обновить» происходит скачивание файла.	
			3. Фейк «Обновление Flash Plaver»	
			Принцип работы:	
			1) Человек заходит на сайт и спустя пару секунд появляется модальное окно в стиле Flash Player, в котором говориться что вышла новая версия и нужно обновиться	
			 После нажатия на «Обновить» происходит скачивание файла. 	
			Все методы разводок адаптивные под мобильный устройства, а также кроссбраузерные и кроссплатформенные.	
			В скрипт встроен перевод на 30 языков и текст в разводке будет автоматически переводиться на язык посетителя.	
			Также в скрипте присутствует фильтрация ботов.	
			Встроен фильтр MacOS , UNIX, Linux, IOS.	
			Скрипт определяет такие языки:	

Historical data from our TI&A system: the landing page in question was first put up for sale as early as January 2018.

In late 2019, the project was shut down and made publicly available, which meant that anyone could download it for free.

12.12.2019 02:20	<mark>Инстал-Пак</mark> Translated: Install-Pak ⊕ exploit.in 12.12.2019 —07.07.2020	F 8	В виду того что сервис закрылся (лоріс/13328/), хочу выложить Инстал Пак (без обфускации и привлахи) + Инструкция в архиве Линк : https://www.sendspace.com/file/kh0fyp маленькое дополнение : Пользуйтесь на здоровье, а то некоторые начали его перепродавать уже) Translated: Since the service has closed (/ topic / 13328 /), i want to post Inst Pak (without obfuscation and binding) + Instruction in the archive Link: https://www.sendspace.com/file/kh0fyp small addition: Use it for health, otherwise some have started to resell it already) @ DR.PREDATOR	^
Details Reliability: 71% Message details	Credibility: 100% Admiralty code: TLP:			
Nickname DR.PREDATOR Messages 1153 Avatars – Telegram @DR_PREDAT E-mail Too many con Phone –	Source exploit.in First message Last message 24.06.2017 31.07.2020 OR @exploit @YUG07824 @myself		Торіс лате Инстал-Пак В виду того что сервис закрылся (лоріс/133328/) хочу выложить Инстал Пак (без обфускации и привязки) - Инструкция вархиве Лими:: http://www.sendsgace.com/file/khôfyp маленькое дополнение: Пользуйтесь на здоровье ја то некоторые начали его перепродавать уже)	TRANSLATE

In late 2019, the user DR.PREDATOR made the landing page publicly available. "Because the service has closed (...), I would like to publish Install Pack (with no obfuscation and binding) + Instructions in an archive (...) Enjoy, because some have already started reselling it"

The structure of the published project is extremely similar to what xxbtc offers. Since October 10, 2019, however, xxbtc has been offering a set that includes the script from DR.PREDATOR.

Details Reliability: 71% Credibility: 80% Admiralty code: TLP: Message details Identical re-posts Identical Nicknames							
Nickname xxbtc Messages 6 Avatars – Telegram @xengi E-mail xxxbtc@exploit.im Phone –	Source opencard.pw First message 17.03.2019	Last message 10.10.2019		Торіс пате Скам, сайты для выдачи вашего exel АКТУАЛЬНО ПОСЛЕДНИЕ ДНИ ПРОДАЮ КОМПЛЕКТІ ИЗ Т 15 сайтов на выдачу ехе разных тематик • Окрипт для exe/apk инсталов от di predator ==== 70\$ Telegram @xengf Corлaceн на гарант!	TRANSLATE		

An amazing coincidence: xxbtc also published a pack that included DR.PREDATOR's script. "Scam websites for delivering your exe! LAST DAYS OF THE OFFER. I AM SELLING A SET OF 15 websites for delivering exe with different topics + a script for exe/apk from dr.predator (...) Telegram @xengf

What does the landing page distribute?

At the time of our analysis, it was established that one of the campaigns involving this landing page distributed several types of malware called RedLine Stealer. We will return to this later.

The campaign involves the following domains:

As can be seen, two bitbucket.org repositories were used for downloading:

https://bitbucket[.]org/FlashPlayerUpdate/flashplayer

https://bitbucket[.]org/AdobeFlashUpdate/flashplayer

Below are screenshots taken on April 19, 2021 showing the two repositories.

The download links led to a file and a malware-containing archive.

FlashPlayer.exe (from the zip file) - SHA1 1ea09cd229b34951007f81c8e5acd323386e4fb6

FlashPlayer.exe - SHA1 36d08c8ab8e161923403cd89bdf3600fccd6629a

Detonation in Group-IB THF Polygon, our system for launching malware in an isolated environment, revealed that these files are samples of RedLine Stealer.

FlashPl PE32 ex 245657	layer.exe xecutable (GUI) Intel 80386 Mono/.Net assembly, for I 76 B			Malicious 83%	
File info Added Processing time Repor User comment Redline from zip	prted	Reliability: Credibility: Admiralty code: A2 TLP:	100% 90%		
Polygon Report / b1ddc0c6df1dae6fa18ed6	6fd948648a48a70f7c8fde63d86aca545b2c850595b 83.6% Probability Known File Names FlashPlayer.exe MD5 / SHA1 / SHA256 1ea09cd229b34951007f81c8e5acd32	File Size 2456.6 kB File Type 23386e4fb6 PE32 executable (GUI) Im mbly, for MS Windows	Proces Interne el 80386 Mono/.Net asse • Avail:	sed at t-connection able	lcon
Behavioral markers Malicious [5] Other [7] Marker					Indicators

Identifying the type of malware: The screenshot shows the result of detonating the files in Group-IB THF Polygon, our system for launching malware in an isolated environment. The files are RedLine Stealer samples.

When executed, the files send the following type of HTTP requests to their command-and-control (C&C) server:

URI	Data
http://checkip.amazonaws.com/	GET / HTTP/1.1 Host: checkip.amazonaws.com Connection: Keep-Alive
http://168.119.153.70:35200/IRemotePanel	POST /IRemotePanel HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/GetTasks" Host: 168.119.153.70:35200 Content-Length: 1021944 Expect: 100-continue Accept-Encoding: gzip, deflate
http://168.119.153.70:35200/IRemotePanel	POST /IRemotePanel HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/GetSettings" Host: 168.119.153.70:35200 Content-Length: 136 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
http://168.119.153.70:35200/IRemotePanel	POST /IRemotePanel HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/SendClientInfo" Host: 168.119.153.70:35200 Content-Length: 1093828 Expect: 100-continue Accept-Encoding: gzip, deflate

In summary, so far our analysis revealed that:

The FontPack landing page is a set of fake webpages designed for tricking users into downloading a malicious file.

FontPack is distributed as a JS script.

The JS script can be installed on a compromised or threat actor-controlled server.

FontPack contains fakes mimicking a browser, font or Adobe Flash Player update.

FontPack works on both desktops and mobile browsers.

The aim of the landing page is to determine what browser version is used and, based on that information, to provide a link for downloading a particular file.

One of the analyzed campaigns involved delivering RedLine Stealer.

What is RedLine Stealer capable of?

The hacker community learned about RedLine Stealer in early 2020, when it was put up for sale for the first time on multiple underground forums.

Message details Identical re-posts Identical Nicknames				
Nickname Glade	Source wwh-club.net			Topic name TRANSLATE REDLINE STEALER
Nickname Glade Messages 253 Avatars Commany contacts! E-mail - Phone -	Source wwh-club.net First message 19 02:2020	Last message 14.01.2021		Торіс лалю тялько и только сюда https://t.me/REDLINESUPPORT и трябовать подтверждение через ЛС форума Хочу представить вам стиллер, заточенный под удобную работу с логами. Собирает максимально-востребованную информацию для работы по всем направлениям. Програмам пасалась с учетом всех пожеланий людей профессионально занимающимися в офере кардинга. Возможностт билда: 1) Собирает и в браузеров: а) Логин и пароли b) Кули c) Поляр автозалолнения d) Кредитные карты c) Поляр автозалолнение карты c) Поляр автозалолнения d) Кредитные карты c)
				 a) Download - загрузка файла по прямой ссылке в указанный путь b) RunPE - инжект 32-битного файла, скачанного по прямой ссылке, в другой файл, который вы укажите

The first post about selling RedLine Stealer made on an underground forum on February 19, 2019

RedLine quickly became popular and has involved over 230 C&C servers since October 2020 according to our data. The stealer is written in C# and its functionality is typical for this type of malware:

1

It collects credentials, cookies, autocomplete field data, and credit card information from all Chromium/Gecko-based browsers

2

It collects data from FTP and IM clients

3

It identifies countries where the stealer will not function

It collects information about the victim's PC

5

It manages anti-duplicate logs settings in the admin panel

6

It deletes itself

7

It performs tasks in four different ways:

These ways are:

- 1. It downloads a file to a specified path through a direct link
- 2. It injects a 32-bit file downloaded through a direct link into another file, which must be specified
- 3. It downloads a file to a specified path through a direct link and later launches it
- 4. It opens a link in the default browser

Interestingly, websites compromised as early as February 2021 still deliver payloads despite the stealer's C&C server no longer being available.

As a closing remark, the campaign is only one of many that involve this landing page. The fake updates are especially interesting considering that Flash Player support was discontinued in early 2021.

Attacks involving the FontPack landing page MITRE ATT&CK and MITRE Shield

Tactics Mitigations & Active Techniques **Techniques Group-IB** of adversaries Defense mitigation & protection products Techniques Techniques Group-IB Tactics Mitigations & Active Defense of adversaries mitigation δ protection products Resource T1583. Acquire Infrastructure M1056. Pre-compromise Threat Intelligence δ Development T1584. Compromise Infrastructure M1016. Vulnerability Attribution T1588.001. Obtain Capabilities: Scanning Security Assessment Malware Initial T1189. Drive-by Compromise M1049. Antivirus/Antimalware Threat Intelligence δ T1190. Exploit Public-Facing Access M1050. Exploit Protection Attribution M1031. Network Intrusion Prevention Application Cyber Education M1016. Vulnerability Scanning M1021. Restrict Web-Based Content Security Assessment M1017. User Training M1051. Update Software DTE0035. User Training DTE0027. Network Monitoring Threat Hunting Framework T1059. Command and Scripting Execution M1049. Antivirus/Antimalware **Threat Hunting Framework** Interpreter T1204. User Execution M1038. Execution Prevention Red Teaming Incident Response M1021. Restrict Web-Based Content M1026. Privileged Account Management DTE0035. User Training DTE0021. Hunting Fraud Hunting Platform DTEO018. Detonate Malware DTEO007. Behavioral Analytics T1036. Masquerading T1027. Obfuscated Files or Defense Evasion DTE0003. API Monitoring Information DTE0034. System Activity Monitoring T1555. Credentials from Password Credential M1049. Antivirus/Antimalware **Credential Access** DTE0007. Behavioral Analytics Access Stores Threat Hunting Framework DTE0003. API Monitoring T1552. Unsecured Credentials DTE0034. System Activity Monitoring Collection T1005. Data from Local System Command T1071. Application Layer Protocol M1038. Execution Prevention **Threat Hunting Framework** and Control T1573. Encrypted Channel M1031. Network Intrusion Prevention DTE0021. Hunting DTE0022. Isolation DTE0027. Network Monitoring DTE0003. API Monitoring DTE0034. System Activity Monitoring DTE0031. Protocol Decoder Group-IB, 2021

Indicators of compromise

Share

Receive insights on the latest cybercrime trends

GROUP