Swascan
TINEXTA CYBER

GANG RANSOMWARE

MARZO 2022

INDICE

INTRODUZIONE

Ad inizio 2022, il ransomware si conferma il malware preferito dalle gang. Con banche statali e agenzie militari prese di mira. I recenti attacchi guidati dalla Russia in Ucraina hanno portato la questione della sicurezza informatica in prima linea, esponendo vulnerabilità ai massimi livelli. Di conseguenza, più agenzie governative di sicurezza informatica hanno rilasciato avvisi al settore finanziario per rafforzare le difese informatiche in previsione di attacchi informatici sempre più ampi.
Ad oggi, per le forme più prolifiche di ransomware, bastano meno di cinque minuti per crittografare 100.000 files, dimostrando quanto velocemente questo può causare una grave crisi di sicurezza informatica per la vittima di un attacco.

LE GANG RANSOMWARE PIÙ ATTIVE

Ma andiamo a scoprire quali sono le gang ransomware che si sono distinte a marzo 2022:

1.LockBit (aka Bitwise Spider)

Cyber gang **russa** nata nel settembre 2019, rinominata nel giugno 2021 **"LockBit 2.0".** Il gruppo compromette le reti delle vittime attraverso una varietà di tecniche, tra cui, ma non limitato a, utilizzo di insider ed exploit zero day. Nel 2021, LockBit 2.0 si è reso responsabile di attacchi di alto profilo, includendo vittime come Accenture. La gang è cresciuta fino a diventare il gruppo leader per il maggior numero di vittime pubblicate sul loro sito darkweb, superando Conti ad inizio 2022.

2.Conti

La gang **Conti** ransomware nasce dal gruppo hacker **russo** Wizard Spider, creatore del famoso ransomware Ryuk, che si ritiene abbia legami con l'intelligence russa. Con un'estorsione di 180 milioni di dollari alle sue vittime nel 2021, la gang Conti era considerata la più pericolosa al mondo, superando di gran lunga i guadagni di tutte le altre gang di ransomware, primato mantenuto fino alla dichiarazione pro-Putin.

3.BlackCat (aka ALPHV)

Gang ransomware emersa a metà novembre 2021 che si è rapidamente guadagnata fama per la sua sofisticatezza e innovazione. Noti anche come ALPHV, il gruppo ha confermato essere ex membri della famigerata operazione BlackMatter/ Darkside ransomware.

4.HiveLeaks

Hive o "**HiveLeaks**" è una gang ransomware relativamente nuova che ha fatto la sua comparsa a fine giugno 2021. Come in molti altri casi, anche Hive ruba i file di potenziale interesse prima di avviare la crittografia, così da poter attuare il doppio ricatto. I dati vengono poi pubblicati sul loro sito, spingendo così le vittime a pagare un riscatto.

5.Stormous

Presumibilmente di origine **iraniana**, il gruppo ha iniziato l'attività ad aprile 2021, operando prettamente tramite il loro canale Telegram con attacchi rivolti verso gli Emirati Arabi Uniti. Il 12 gennaio Stormous ha inaugurato un servizio a pagamento di acquisto prodotti di violazione vittime, con prezzo variabile in base alla richiesta. Da marzo 2022, il gruppo è inoltre attivo sotto rete TOR. Tuttavia, poco dopo l'impostazione di tale servizio, il gruppo ransomware Arvin Club ha compromesso il loro sito, facendo trapelare informazioni sensibili.

6. AgainstTheWest (Bluehornet/ Brazeneagle)

AgainstTheWest è un gruppo di hacktivisti attivo da ottobre 2021 e supportati da **Taiwan,** secondo un articolo di Wikipedia in lingua inglese. La gang ha effettuato una serie di attacchi informatici contro organizzazioni in Cina, tutti avvenuti tra ottobre e novembre 2021.

7.Blackbyte

Gruppo nato nel luglio 2021 con attacchi principalmente rivolti contro Stati Uniti, Europa e Australia. Mesi dopo, la banda è stata colpita da un momento difficile, quando la società di sicurezza informatica Trustwave ha rilasciato uno strumento di decriptazione che ha permesso alle vittime di BlackByte di recuperare i loro file gratuitamente. Le tecniche semplicistiche di crittografia del gruppo hanno portato alcuni a credere che il ransomware fosse opera di dilettanti; tuttavia, si è attestato il ritorno dopo aver preso di mira almeno tre settori di infrastrutture critiche statunitensi, secondo un avviso da parte dell'FBI e dei servizi segreti[1].

8. Vice society

Gang relativamente nuova, emersa a giugno 2021 lanciando attacchi a vittime di piccole e medie dimensioni. La banda è nota per l'utilizzo della doppia estorsione, rivendicando attacchi a diversi distretti scolastici, tra cui il Manhasset Union Free School District a Long Island e centri medici come United Health Centers of San Joaquin Valley, in California, attacchi che sembrano esaltare l'assenza di etica o morale nella scelta dei target da prendere di mira.

9. Pandora

Il gruppo **Pandora** è un nuovo player che si è aggiunto allo spazio ransomware all'inizio di marzo 2022. Si tratta della versione rinominata di Rook ransomware. Un gruppo di criminal hacker che si sta facendo strada, rivendicando la responsabilità del furto di informazioni aziendali sensibili di Denso, importante fornitore di parti di ricambio del gruppo Toyota Motor Corp., minacciando di rivelare pubblicamente le informazioni interne dell'azienda il 16 marzo.

10. Karakurt

Gruppo di criminalità informatica di nuova costituzione che in pochi mesi ha colpito un gran numero di vittime. Caratteristica distintiva è la deviazione dall'approccio tipico di presa di mira di grandi aziende o servizi di infrastrutture critiche, optando per un approccio più veloce in cui compromettono aziende di piccole dimensioni o filiali aziendali. Questo consente alla gang di passare alla prossima vittima più velocemente.

11. Suncrypt

La gang **SunCrypt** ha iniziato a condurre attacchi ransomware nell'ottobre 2019. È considerata la prima gang ad avere introdotto attacchi ransom DDoS (RDDoS) come tattica di estorsione utilizzata in combinazione con attacchi ransomware aziendali.

12. Lapsus$

Si tratta di un gruppo relativamente nuovo che ha iniziato a farsi notare lo scorso dicembre, caratterizzato da un'intensa presenza su Telegram. Si differenzia da altre gang di cyber criminali per i suoi attacchi ransomware non tradizionali, limitandosi alla fase del furto di dati e all'estorsione, senza la criptazione dei dati delle vittime, alle cui macchine accede tramite phishing. La gang si sta facendo strada nel settore prendendo di mira obiettivi di alto profilo, tra cui Samsung e Nvidia, causando pesanti leak.

13. Everest

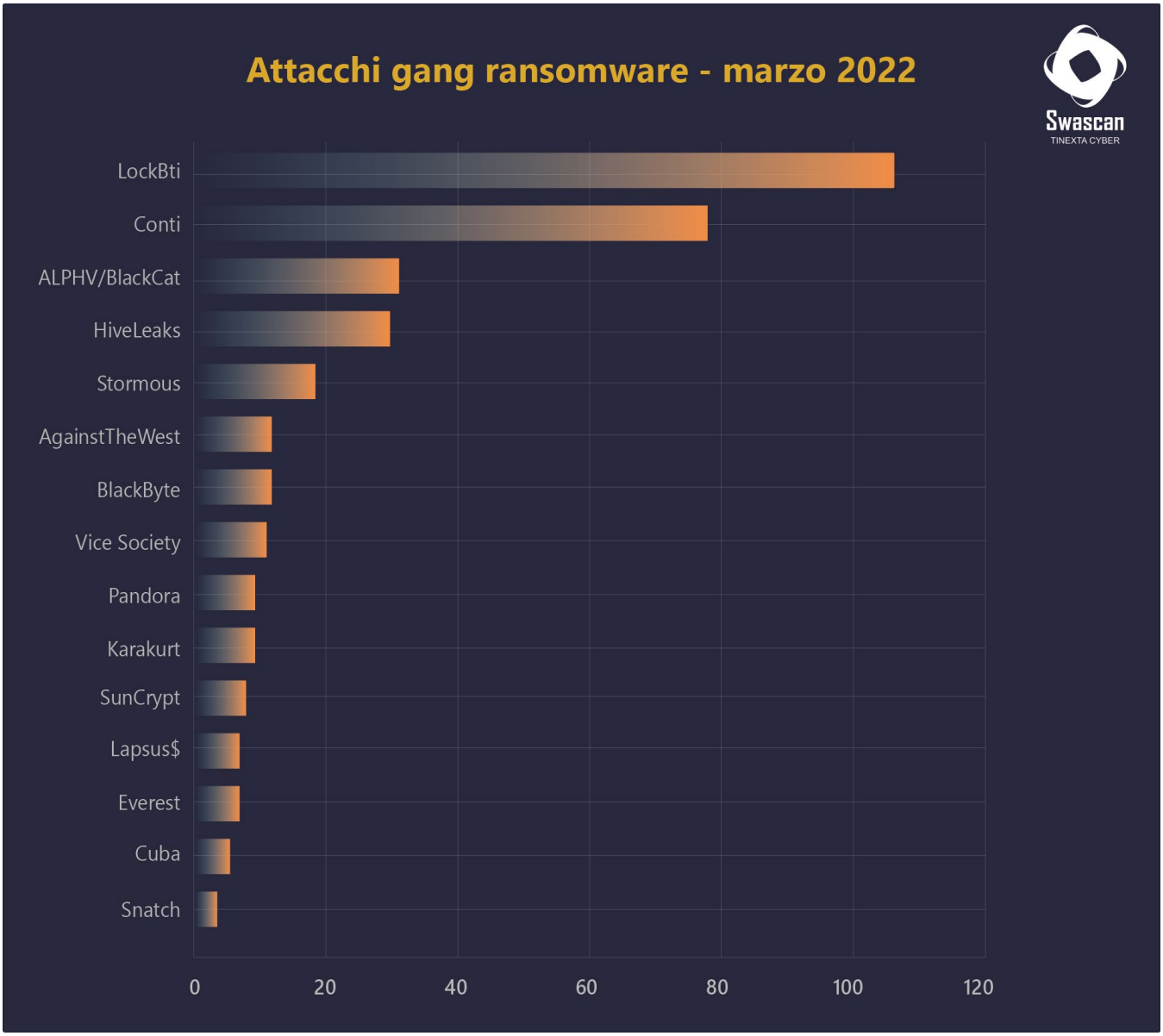
Gang ransomware relativamente recente, comparsa nel dicembre 2020. Nota soprattutto per l'attacco alla SIAE (ottobre 2021), la Società Italiana Autori ed Editori, della quale sono stati pubblicati i dati personali relativi agli associati (soprattutto cantanti).

14. Cuba

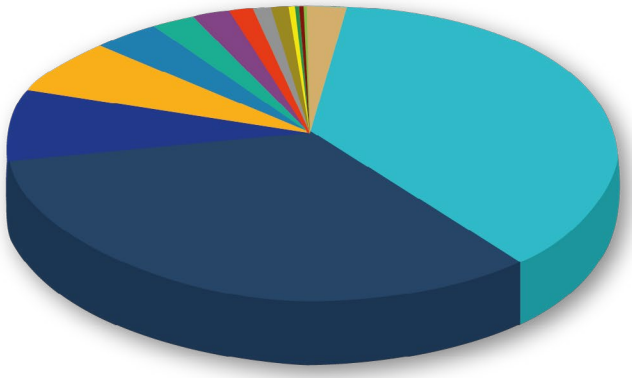
comparsa per la prima volta alla fine del 2019, nonostante il nome del gruppo lasci pensare alla provenienza, in realtà si presume siano basati in Russia. Vittime della gang includono (ma non sono limitati a) organizzazioni nei settori finanziario, governativo, sanitario, manifatturiero e informatico.

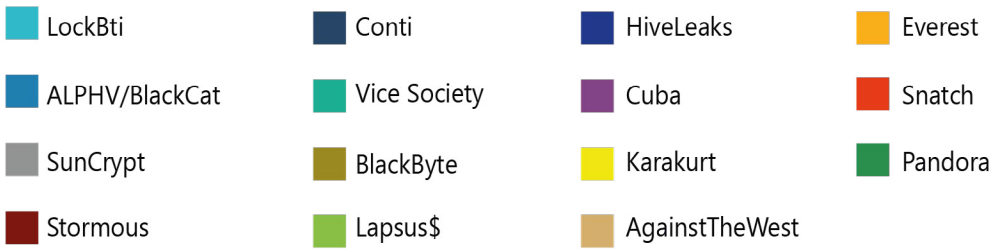
15. Snatch

Gang attiva da dicembre 2019 con operazioni di estorsione singola, si è evoluta nel 2021 con pratiche di doppia estorsione e con furti massivi di dati, confermando un gran numero di vittime in pochissimi mesi.


Attacchi gang ransomware - marzo 2022
Swascan
TINEXTA CYBER
LockBti
Conti
ALPHV/BlackCat
HiveLeaks
Stormous
AgainstTheWest
BlackByte
Vice Society
Pandora
Karakurt
SunCrypt
Lapsus$
Everest
Cuba
Snatch
0
20
40
60
80
100
120

Totale Attacchi Ransomware





Vittime Globali Ransomware - Marzo 2022

Totale vittime: 331

Paesi attaccati: 64

GUERRA RUSSIA - UCRAINA:
Le gang ransomware si schierano sul fronte cyber

Fin dall'inizio della **guerra tra Russia e Ucraina**, molti l'hanno definita la prima guerra ibrida su ampia scala[2] , in quanto coinvolge sia attacchi informatici che sul campo. Già giorni prima che le prime forze russe entrassero in Ucraina secondo fonti Eset, le gang informatiche legate alla Russia hanno preso di mira siti ucraini[3] .
Tuttavia, questi erano solo i primi di una lunga serie di attacchi che hanno dato vita ad una cyberwar invisibile nei forum del darkweb. Difatti, oltre all'utilizzo di social network per comunicare con il pubblico, molti di questi gruppi si sono rivolti al darkweb come spazio sicuro per coordinare attacchi contro siti specifici russi o ucraini.

In questa guerra cibernetica attacchi di tipo APT (Advanced Persistent Threat) sono ormai considerati strumento di primo piano per il perseguimento di interessi politici, economici e militari, portati avanti da dozzine di collettivi come hacktivisti, gruppi di hacker e gang ransomware conosciute che solitamente agiscono opportunisticamente per estorcere ingenti somme di denaro alle vittime. Molti di loro si sono schierati con la Russia o l'Ucraina nelle ultime settimane.

Da una parte, dunque, gli attori filo-ucraini che si rifiutano di vendere, comprare o collaborare con alleati russi schierandosi a sostegno dell'Ucraina; dall'altra invece, gli attori filorussi, si stanno sempre più focalizzati nella battaglia contro gli oppositori russi.

Dopo un'attenta analisi, si è riscontrato l'utilizzo di forum darkweb per il rilascio di informazioni sensibili appartenenti alla nazione nemica, compresi quelli delle agenzie governative e militari, organismi politici, aziende pubbliche e private, così come numerosi annunci richiedenti donazioni a favore dell'Ucraina. Allo stesso modo, questi forum si caratterizzano per discussioni e pianificazione di attacchi futuri, coinvolgendo direttamente le persone incitandole a rifiutare di comprare, vendere o collaborare con alleati russi o ucraini.

Partendo dall'analisi relativa alle gang ransomware che si sono distinte nel mese di Marzo, riportiamo di seguito una tabella con lo schieramento sul fronte cyber di ciascuna gang nella guerra Russia - Ucraina, laddove dichiarato:

GANG	PRO RUSSIA	PRO UCRAINA	NON SPECIFICATO
LockBit			x
Conti	x		
ALPHV/BlackCat			x
HiveLeaks			x
Stormous	x		
AgainstTheWest		x	
BlackByte			x
Vice Society			x
Pandora			x
Karakurt			x
SunCrypt			x
Lapsus$			x
Everest			x
Cuba			x
Snatch			x

A febbraio, la gang **Conti** si è ufficialmente schierata con la Russia pubblicando un annuncio sul suo data-leak-site (DLS), annunciando "supporto totale" attraverso "tutte le risorse disponibili".

Figura 1: Conti si schiera con la Russia (screenshot del messaggio originale postato sul sito darkweb della gang, successivamente modificato come riportato di seguito)

Tuttavia, il messaggio sembra aver causato dissenso, motivo per cui il gruppo ha successivamente modificato il messaggio per rimuovere la minaccia contro le infrastrutture critiche:

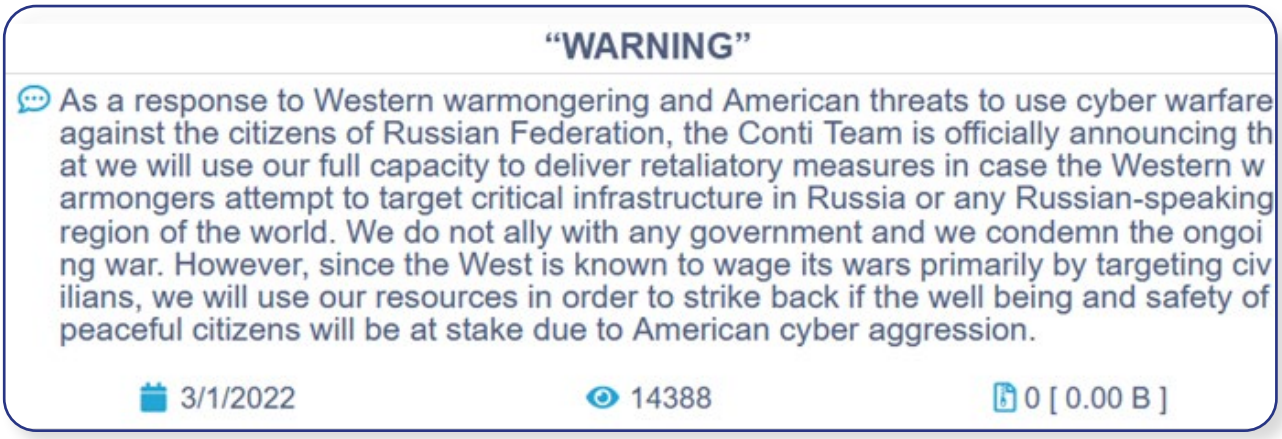


Figura 2: Conti, dichiarazione rivisitata (ritirando parte del forte linguaggio utilizzato precedentemente, minacciando un contrattacco solo se infrastrutture critiche in Russia o nei paesi vicini fossero state prese di mira)

Poco dopo la dichiarazione di sostegno della gang Conti, quest'ultima ha subito una devastante violazione da parte di un security researcher ucraino con conseguente divulgazione del codice sorgente del Team Conti, delle TTP (tattiche, tecniche e procedure) e delle comunicazioni interne del gruppo.
Il membro infiltrato del gruppo criminale di ransomware Conti ha reso pubbliche le informazioni tramite account Twitter @ContiLeaks, con rilascio di più versioni del codice sorgente[4] .

Nei documenti svelati ci sono almeno un anno di conversazioni sottratte all'applicazione di messaggistica open-source Jabber: la chat fornisce illuminanti spiegazioni su come Conti operi di giorno in giorno, come ricicli i propri riscatti attraverso le criptovalute e, soprattutto, collegano direttamente i membri del gruppo Conti alle agenzie di spionaggio russe.

Figura 3: Rilascio di informazioni sul forum XSS

Per quanto riguarda **LockBit**, si nota come nel darkweb gli attacchi sono rivolti a vittime di un po' tutte le nazionalità. Tranne alla Russia e paesi vicini. Come analizzato dal ricercatore Will Thomas, LockBit controlla le lingue del sistema per evitare la crittografia delle macchine in Russia e nei paesi vicini. La gang risolve le funzioni GetSystemDefaultUILanguage e GetUserDefaultUILanguage e le chiama a verificare se il sistema o l'utente utilizzano una lingua presente nella lista da evitare qui sotto:

```
result = (unsigned __int16)GetUserDefaultLangID();
if ( (_WORD)result == 0x82C                    // Azerbaijani (az)
  || (_WORD)result == 0x42C                    // Azerbaijan, Latin (AZ)
  || (_WORD)result == 0x42B                    // Armenian (hy)
  || (_WORD)result == 0x423                    // Belarusian (be)
  || (_WORD)result == 0x437                    // Georgian (ka)
  || (_WORD)result == 0x43F                    // Kazakh (kk)
  || (_WORD)result == 0x440                    // Kyrgyz (ky)
  || (_WORD)result == 0x819                    // Russian (Moldova)
  || (_WORD)result == 0x419                    // Russian (ru)
  || (_WORD)result == 0x428                    // Tajik (tg)
  || (_WORD)result == 0x442                    // Turkmen (tk)
  || (_WORD)result == 0x843                    // Uzbek (uz)
  || (_WORD)result == 0x443                    // Uzbekistan, Latin (UZ)
  || (_WORD)result == 0x422 )                  // Ukrainian (uk)
{
  ExitProcess(0);
}
```

Tuttavia, prendere una posizione ha delle conseguenze, come abbiamo notato con la gang Conti. Questo ha portato la gang **LockBit** a negare ogni tipo di azione attiva o complementare per quanto riguarda la guerra che si sta svolgendo tra Ucraina e Russia. In un comunicato hanno affermato:

> *"La nostra comunità è composta da molte nazionalità del mondo, la maggior parte dei nostri pentesters sono della CSI tra cui russi e ucraini, ma abbiamo anche americani, inglesi, cinesi, francesi, arabi, ebrei, e molti altri nel nostro team. I nostri programmatori sviluppatori vivono permanentemente in tutto il mondo in Cina, Stati Uniti, Canada, Russia e Svizzera. I nostri server si trovano in Olanda e alle Seychelles, siamo tutte persone semplici e pacifiche, siamo tutti terrestri. Per noi è solo business e siamo tutti apolitici. Siamo interessati solo al denaro. Non prenderemo mai, in nessuna circostanza, parte a cyber-attacchi alle infrastrutture critiche di qualsiasi paese del mondo o ci impegneremo in qualsiasi conflitto internazionale."*

("Official Statement on the Cyber Threat to Russia", LockBit darkweb site)

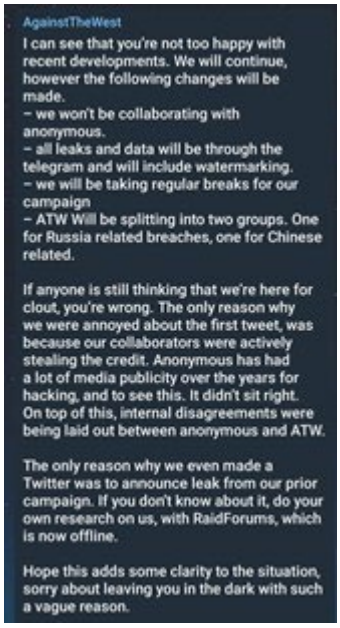
Un altro gruppo, **ALPHV**, si afferma "estremamente rattristato" dal comportamento di Conti, condannandolo. Anche loro come LockBit si dichiarano neutrali, affermando che nel loro business non ci sono nazionalità o altre ragioni che possano giustificare l'uccisione. Aggiungono, inoltre, che Internet, e in particolar modo il darkweb, non è un posto per politici.

AgainstTheWest, schierato pro-Ucraina, ha rivendicato l'attacco alla **Banca Centrale di Russia**, esfiltrandone dati, così come al **Russia Aerospace Force**, compromettendone la video sorveglianza remota, ma anche al servizio di meteorologia e monitoraggio ambientale della Russia.

Il gruppo ha anche postato sul suo canale Telegram la violazione con successo di una società russa di sicurezza informatica:

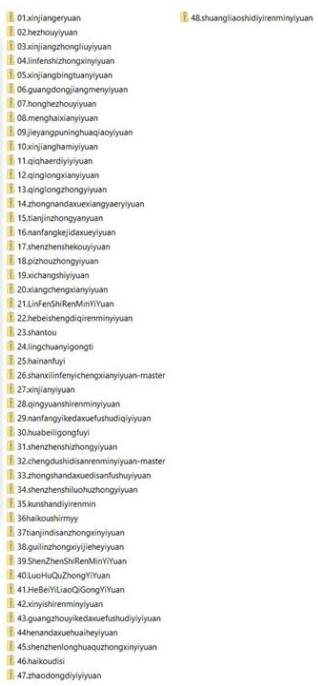
A partire dal 1 marzo, la gang ha rilasciato nuove dichiarazioni sul suo canale Telegram e su un forum darkweb per ulteriori chiarimenti:

"Non collaboreremo con Anonymous". Inoltre, *"ATW sarà diviso in due gruppi. Uno per violazioni legate alla Russia, uno per quelle legate ai cinesi"*, aggiungono.



Partial List of Notable Chinese Data Breaches (there have been more than 200):	Some Notable Russian Government Data Breaches:
Alibaba Cloud (3 times)	Russian Space Forces
Bank Of China	AIP of the Russian Federation
Huawei	PJSC Aeroflot (Russia Airlines)
China Petroleum Technology & Development Corporation	Ministry of Digital Development, Communications and Mass
Chinese Prisons	Media of the Russian Federation, Pskov Region
China Oil	Ministry of Emergency Situations of the Russian Federation
Ministry Of Justice China	Federal State Statistics Service
WeChat	Federal Service for Labour and Employment (Ministry of Labor
Tencent	and Social Protection of the Russian Federation)
Starbucks China	Novolipetsk Steel
Xiaomi Cloud	Sberbank
Ministry Of Public Security	DNPP
Lenovo China	ROSHYDROMET
China's Hunan Government	Belarusian Media CTV
JD.com	AMD Russia
Amazon China (Privated)	BrandSquad Russia
Center for Disease Control and Prevention	Delans Russian Postal
Ministry of Public Security	Development of Territories of the Russian Academy of Sciences
Ministry of Science and Technology	Federal State Budgetary Educational Institution of Higher
State Market Regulatory Administration	Education Altai State Pedagogical University of the Russian
cable maker Zhongtian Technology Submarine Cable Co	Federation
	Gazprom
	Nauchnyy Tsentr Prikladnoy Elektrodinamiki
	OJSC Ak Bars Holding
	PromEngineering
	Russia Air
	Russian Rail

Il gruppo ha intensificato i suoi attacchi contro bersagli cinesi, violando con successo la società di e-commerce Alibaba, rilasciando 30GB di materiale, e rendendo pubblico un database del Ministero della Salute della Repubblica Popolare Cinese, per un totale di 3.313 files e 603 directories. Entrambi sono stati condivisi in un forum dark web.



La gang ha continuato la sua offensiva contro cyber gang cinesi, nordcoreane e russe e i loro membri. Rilasciando un file su Telegram e sul darkweb, il gruppo ha reso pubblici nomi, indirizzi e-mail, social e account Github, dati della carta di credito, e altre informazioni identificative dei partecipanti dei gruppi insieme ad altre rivelazioni scioccanti. Alcune includono:

APT38: Cina e Corea del Nord hanno collaborativamente avuto una talpa all'interno del Congresso degli Stati Uniti dal 2011.

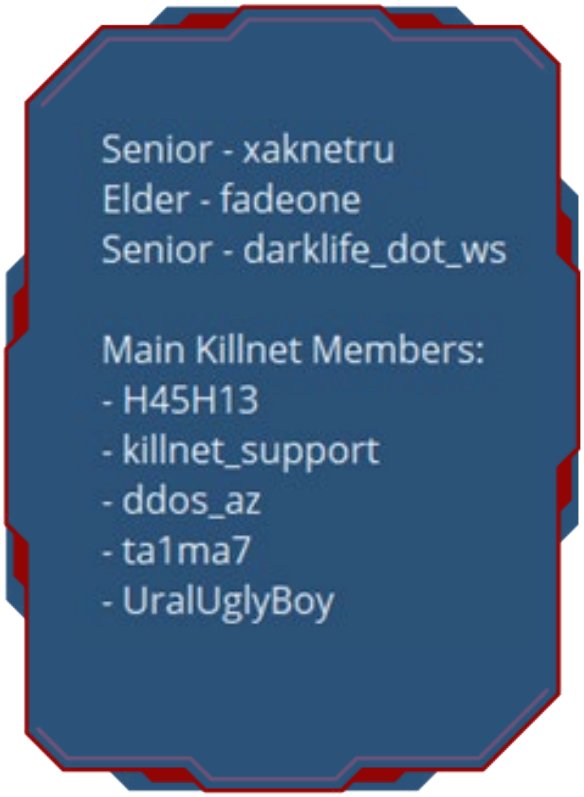
APT3: Threat actors strettamente allineati con dipendenti di Tencent - il gigante tecnologico cinese dietro WeChat e QQ.

APT38/APT3: L'alias "ph4nt0m" appare nelle informazioni per entrambi i gruppi e si ritiene sia affiliato con APT17 dalla Cina.

APT40: Threat actors collegati casualmente ai dipendenti di ByteDance, la società madre di TikTok.

ATW ha inoltre preso di mira la cyber gang pro-russia KILLNET, pubblicando un documento contenente le informazioni personali di membri chiave russi, con relativi social media, informazioni di contatto e associazioni familiari.


[Social Media Accounts]
VK: id14503478 (Deleted)
Skype: d.makarov | Scaramoush777 | live:d12345691 | live:.cid.c43777a7aaaa879b | dmitriyy.badin
Instagram: https://www.instagram.com/dmitry.badin/
Gravatar: http://en.gravatar.com/demorales524
Facebook: https://www.facebook.com/dmitriyy.badin
Instagram: https://www.instagram.com/badin.dmitriy75972018/
Habr: https://career.habr.com/dmitriybadin
WebFlow: https://webflow.com/4322221
[Phone Details]
In-Use Number: +79535585216
Country Code: +7 (RU)
SIM provider: LLC T2 Mobile
Old Numbers: +79261291279 | +8(926)129-1279
[Location Details]
Current City: Nizhny
Current District: Novgorod
Current Country: Russia
[IP Information]
Current IP: 46.8.48.112
Current ISP: ZagorodTelecom LLC
Previous ISPs: PJSC Vimpelcom
Previous IPs: 76.32.74.133 | 95.28.153.94 | 163.106.144.169
[Family Details]
Personal title: Wife
Full legal name: Viktoria Dzyubenko
VK.com: https://vk.com/id44404910
DOB: 11 December 1988


Senior - xaknetru
Elder - fadeone
Senior - darklife_dot_ws
Main Killnet Members:
- H45H13
- killnet_support
- ddos_az
- ta1ma7
- UralUglyBoy

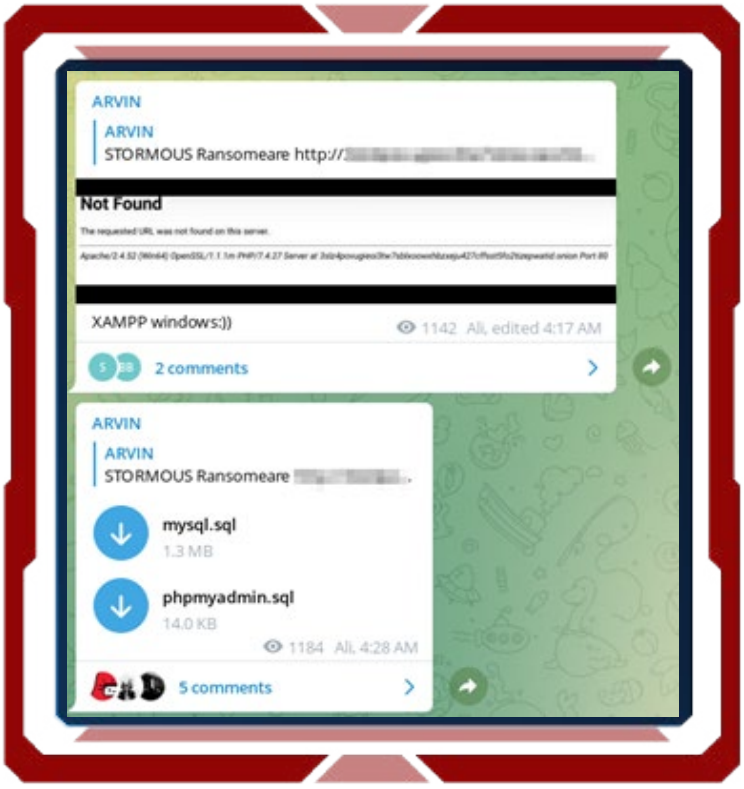
STORMOUS (a.k.a. Stormus, Stourmous), scende in campo con i russi.

Dall'inizio dell'invasione ucraina, la gang Stormous ha attirato l'attenzione su di sé intensificando le proprie azioni unicamente verso target USA, EU e Ucraina, destando i primi sospetti di supporto al governo russo, ipotesi poi confermate il 01/03 con l'ufficialità dello schieramento pro-Russia sul loro canale Telegram e relativi attacchi verso le strutture strategiche Ucraine. In uno dei loro post Telegram, infatti, Stormous si attribuisce un DDoS mirato al sito web del Ministero degli Affari Esteri dell'Ucraina.

> *"Their network is fragile – their various data has been stolen and distributed according to their phone numbers, email, accounts, and national card numbers with an internal network hacked and access to most essential files. this is with placing denial attacks on their main site!"*

Tuttavia, è stato osservato che il sito web era già irraggiungibile. L'8 marzo, la società israeliana di sicurezza informatica Kela ha affermato che Stormous ransomware stava falsamente rivendicando la responsabilità per le operazioni che altri attori avevano effettivamente effettuato.

Come già anticipato, poco dopo che la gang ha iniziato ad operare su Tor, il gruppo ransomware Arvin Club ha compromesso il loro sito facendo trapelare database SQL e informazioni riservate. Non è chiaro se questo attacco sia avvenuto a causa della fedeltà russa di Stormous o se Arvin volesse semplicemente dare ai cyber criminali una lezione nella creazione di siti sicuri sul DarkNet.



Ma Stormous non si ferma: sul loro sito darkweb dichiarano di aver colpito INFOTECH, compagnia di sicurezza e videosorveglianza con base in Ucraina, e mettono in guarda la Francia per quanto riguarda le minacce alla Russia.

CAPACITA' CYBER RUSSIA E UCRAINA

Da un lato l'Ucraina, che, come afferma Ben Hall, giornalista del Financial Times[5] , soffre di mancanza di competenze in materia di sicurezza informatica, scarsa regolamentazione, capacità di risposta limitata e mancanza di coordinamento tra le diverse agenzie, tutte carenze che Kiev sta cercando di risolvere.

Dall'altro la potenza russa, con un sovraccarico di risorse finanziarie e umane altamente organizzate, capacità informatiche avanzate nel campo della difesa e della deterrenza, in grado di monitorare e rispondere agli attacchi informatici, rilevare lacune nei sistemi nemici e pianificare attacchi efficaci che comportano pesanti perdite.

Le autorità ucraine, pienamente consapevoli delle capacità informatiche russe, si sono quindi impegnate in una corsa contro il tempo per sviluppare le loro capacità nel campo della cyber difesa e della sicurezza, rispondendo agli attacchi con il reclutamento di esperti informatici[6] .

Lo State Service of Special Communications and Information Protection of Ukraine ha tenuto diverse esercitazioni di simulazione di attacchi informatici rivolti a server e reti governative, con lo scopo di sensibilizzare gli operatori delle infrastrutture critiche e metterli in contatto con centri di sicurezza cibernetica, in modo che gli attacchi possano essere rapidamente monitorati e analizzati.

IL RUOLO DEGLI STATI UNITI E DELL'EUROPA

C'è però da considerare che L'Ucraina non è sola: gli Stati Uniti hanno inviato esperti e fondi per rafforzare le difese informatiche dell'Ucraina, e si dichiarano pronti a guidare il fronte cibernetico ucraino e a svolgere compiti difensivi quando necessario.

Una solida prova di questo è stata la dichiarazione del presidente degli Stati Uniti Joe Biden, nel gennaio 2022, avvertendo la Russia delle conseguenze relative agli attacchi informatici, affermando: *"se continuano a utilizzare gli sforzi informatici, beh, risponderemo allo stesso modo".*

Con l'avanzare del conflitto militare, aumenta anche il timore di una guerra informatica senza precedenti, alimentato anche da una lunga serie di attacchi informatici sempre più intensi, tra cui lo storico attacco hacker del 23 dicembre 2025, che fece rimanere gli ucraini senza riscaldamento ed elettricità per diverse ore, o il grave attacco malware russo che nel 2017 ha disabilitato i sistemi del governo ucraino e del settore privato. Gli sforzi di mobilitazione cibernetica da entrambe le parti non si fermeranno.

A causa dell'interconnessione globale, gli attacchi informatici hanno il potenziale di integrarsi nella società tradizionale e causare distruzione diffusa e panico, sollevando prospettive inquietanti.

PREVISIONI SULLA FUTURA ATTIVITÀ DELLE GANG RANSOMWARE

Negli anni passati, la tecnica utilizzata per il ransomware era principalmente quella della singola estorsione, in cui gli aggressori crittografano i dati di un'organizzazione e richiedono un riscatto in cambio di una chiave di decrittazione.
Ora, i gruppi ransomware stanno esfiltrando i dati delle vittime in una posizione offsite prima della crittografia, minacciando quindi la fuoriuscita di dati se un riscatto non viene ricevuto.

La minaccia combinata della crittografia e dell'esfiltrazione dei dati è una forma di doppia estorsione, metodo di attacco sempre più utilizzato e che si dimostra sempre più redditizio. Altra caratteristica di quest'anno sarà la diffusione della tripla estorsione, tecnica concepita per far pagare di più e più in fretta alle aziende, estendendo l'attacco a clienti e partner della vittima.

Attacchi ransomware che diventeranno sempre più mirati, rendendo più difficile per le aziende difendere le loro reti e sistemi. La mossa più urgente da fare è abbassare la soglia di rischio, aumentando la prevenzione.

Inoltre, visti i recenti sviluppi sul piano geopolitico, sarebbe sciocco non considerare come la connivenza tra Cyber Crime e Cyber war siano aumentate enormemente.
Un attacco ransomware - anche se portato a segno da attori non ufficialmente schierati o senza alcuna motivazione politica - è comunque in grado di aumentare indirettamente la potenza di fuoco di un attore statale, proprio grazie alla quantità di dati messi in rete dai primi.
Una nuova realtà scomoda, dove il reame della cyber è adesso appannaggio di due gruppi simili per modus operandi e TTP, ma diversi per obiettivi. Due gruppi che tramite le loro attività si auto-alimentano.

COME OPERA IL RANSOMWARE: CYBER KILL CHAIN

Reconnaissance

Ricognizione dei target

Delivery

Trasmissione dell'arma al target

Installation

Creazione di una via di accesso ai sistemi

Actions on objectives

Svolgimento di azioni mirate all'obiettivo dell'attacco

Weaponization

Individuazione di uno strumento malevolo e delle vulnerabilità attraverso cui sfruttarlo

Exploitation

Utilizzo di una vulnerabilità per entrare nei sistemi

Command & Control

Chiamata al Command & Control

COME DIFENDERSI DAL RANSOMWARE: IL CYBER SECURITY FRAMEWORK

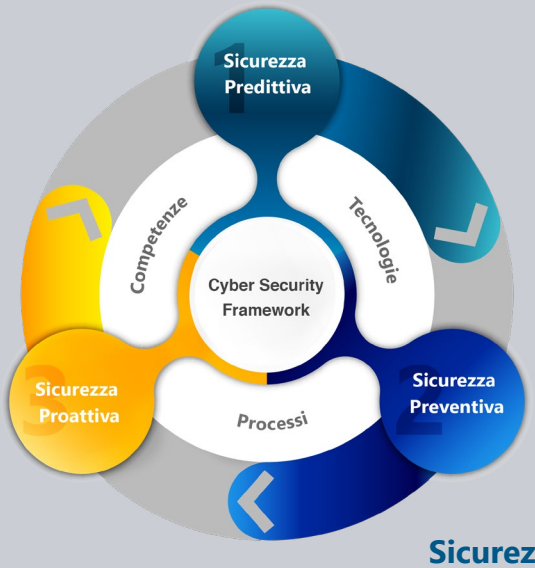
L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno solidificati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**

Swascan
TINEXTA CYBER

Sicurezza Predittiva

1. Identifica le minacce aziendali fuori dal perimetro aziendale operando a livello di web, Darkweb e Deepweb
2. Ricerca eventuali minacce emergenti
3. Effettua attività di Early Warning
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di attenzione alla Sicurezza Proattiva



Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale
2. Contrasta e blocca gli attacchi informatici
3. Gestisce i Cyber Incident
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di investigazione alla Sicurezza Predittiva

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber
2. Definisce i piani di remediation
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva

Sicurezza Predittiva

Domain Threat Intelligence: La Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target. Opera unicamente sulle informazioni disponibili sul web, Darkweb e deepweb. Raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e Closint (Close Source Intelligence) presenti su database, forum, chat, newsgroup.
Nello specifico, in base al dominio-target di analisi, identifica:

- Potenziali Vulnerabilità
- Dettagli delle Vulnerabilità in termini di CVE, impatti e severity
- Impatti GDPR (CIA)
- Numero dei Sottodomini
- Numero Potenziali e-mail compromesse (vengono solo conteggiate e non raccolte o trattate)
- Numero delle Source delle e-mail compromesse
- Typosquatting

Cyber Threat Intelligence: È il servizio evoluto di Threat Intelligence di Swascan. Effettua una attività di ricerca, analisi e raccolta delle informazioni presenti a livello web, Darkweb e Deepweb relativamente al dominio/target di analisi.
Nello specifico:

- Data Leaks: credenziali/source/data
- Identifica Forum/Chat ...
- Botnet relative a dispositive di Clienti, Fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Early Warning Threat Intelligence: È il servizio di Early warning che segnala giornalmente le evidenze che vengono identificate e raccolte nel Darkweb e deep web relativamente al target di analisi.
Nello specifico:

- Data Leaks
- Scraping data
- Phishing data
- Botnet

Sicurezza Preventiva

Tecnologico

Vulnerability Assessment: Esegue la scansione di siti e applicazioni web per identificare e analizzare i modo proattivo le vulnerabilità di sicurezza.

Penetration Test: Le attività di Penetration Test sono svolte da Penetration Tester certificati e in linea con gli standard internazionali OWASP, PTES e OSSTMM.

Human Risk

Phishing/Smishing attack Simulation: Permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso delle vere e proprie simulazioni di attacco. È infatti possibile, attraverso un'interfaccia web inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. I dipendenti, infatti, grazie a questi attacchi simulati riusciranno, in futuro, ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Un'insostituibile attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacco phishing/smishing .

Awareness: Corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di Awareness per il personale tecnico, per i dipendenti e per i Top Manager.

Processo – Compliance

ISO27001: ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano). Dal momento che l'informazione è un bene che aggiunge valore all'organizzazione, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

ICT Security Assessment: L'ICT Security Assessment è una metodologia proprietaria di Swascan che permette alle aziende di verificare e misurare il proprio livello di rischio cyber e di valutare l'efficacia delle misure di sicurezza adottate. Il servizio fornisce le indicazioni e le azioni correttive da adottare a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.

Sicurezza Proattiva

SOCaaS: La progettazione, la messa in esercizio e il mantenimento di un Security Operation Center può essere costoso e complesso. Il servizio **SOC as a Service** Swascan è la soluzione più efficace, efficiente, coerente e sostenibile per i contesti aziendali. Il Soc as a service con il suo servizio di Monitoring & Early Warning permette di **identificare**, **rilevare, analizzare** e segnalare gli attacchi cyber prima che possano trasformarsi in una minaccia concreta per l'azienda.
Un team dedicato nell'attività di **Monitoring & Early Warning** reattivo delle minacce informatiche sulle reti locali, ambienti cloud, applicazioni ed endpoint aziendali. Il nostro team di Security Analyst monitora i dati e le risorse ovunque risiedano all'interno dell'azienda. Indipendentemente dal fatto che le risorse siano archiviate nel cloud, in locale o in entrambi. L'attività di monitoring e segnalazione permette di agire solo quando viene identificata una minaccia reale.

Incident Response Management: è un insieme di risorse e procedure organizzate e strutturate per garantire la corretta reaction e gestione degli incidenti informatici. In caso di incidente informatico, Data Breach, DDoS, attacco Ransomware e/o relativo Data Recovery è necessario affrontare e rispondere con un approccio strutturato, predisposto e organizzato per affrontare in maniera efficace ed efficiente la violazione della sicurezza e per ridurre gli impatti a livello di Business Continuity aziendale. L'obiettivo dell'Incident Response è quello di:

- Gestire l'incidente;
- Limitare i danni diretti e indiretti;
- Ridurre tempi e costi di ripristino.

ABOUT US

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di idetità digitale e sicurezza digitale.

Analysis by:

Martina Fonzo

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI

REFERENZE

1. https://www.ic3.gov/Media/News/2022/220211.pdf

2.https://www.affaritaliani.it/esteri/terza-guerra-mondiale-e--il-primo-conflitto-ibrido-fisico-cibernetico-783914.html

3.https://www.corrierecomunicazioni.it/cyber-security/ucraina-russia-scatta-la-prima-cyberwar-mondiale-a-rischio-ilworld-wide-web/

4. https://twitter.com/vxunderground/status/1505555084452798469

5. https://www.ft.com/content/778997c3-50ce-4b40-9c20-c8564c840a57

6. https://twitter.com/FedorovMykhailo/status/1497642156076511233