

# 다크웹 계정유출 해부하기?

Intelligence-Led Security

윤광택 상무 | Recorded Future

2025년 4월 15일




보안은  
우선순위(prioritization)의  
문제이다.

# 최근 보안 뉴스

oracle cloud traditional hacked (login.(X).oraclecloud.com)  
rose87168 - Thursday March 20, 2025 at 02:40 PM

rose87168  
Yesterday, 02:40 PM (This post was last modified: Yesterday, 02:44 PM by rose87168)



Hello,  
Oracle traditional servers were hacked (domains : login.(region-name).oraclecloud.com )  
Around 6 million user customers' data from SSO and LDAP was stolen.  
JKS files, passwords, key files, and enterprise manager JPS keys were also taken.  
The SSO passwords are encrypted, they can be decrypted with the available files. also LDAP hashed password can be cracked. (I couldn't do it, but if someone can tell me how to decrypt them, I can give them some of the data as a gift.)  
I'll list the domains of all the companies in this leak. Companies can pay a specific amount from the list before it's sold.  
I can also trade for 0-day exploits. send me a private message (PM).  
oracle can send me a message through the company's official email to My Email w/ PM for Offer

Breached

MEMBER

Posts: 2  
Threads: 2  
Joined: Mar 2025  
Reputation: 0

Sample LDAP >  
Company list >  
Sample DataBase >

```
[align=left]* Matt Wallace, users, 11987096172814988, cloud.oracle.com, cn=Matt Wallace, cn=users, orclMNTenantGuid=11987096172814988, dc=oracle, dc=com  
orclMntuid: eFkd-test.matt_wallace@hitchiner.com  
tenantadmin: cn=TenantAdminGroup, cn=Groups, orclMNTenantGuid=11987096172814988, dc=cloud, dc=oracle, dc=com  
userwriteprivilege: cn=orclUserWritePrivilegeGroup, cn=SystemIDGroups, orclMNTenantGuid=11987096172814988, dc=cloud, dc=oracle, dc=com  
userreadprivilege: cn=orclUserReadPrivilegeGroup, cn=SystemIDGroups, orclMNTenantGuid=11987096172814988, dc=cloud, dc=oracle, dc=com  
userwriteprefprivilege: cn=orclUserWritePrefPrivilegeGroup, cn=SystemIDGroups, orclMNTenantGuid=11987096172814988, dc=cloud, dc=oracle, dc=com  
orclMntenantname: eFkd-test  
orclMntenantguid: 11987096172814988  
orclMntenantstate: ENABLED  
orclpasswordold: {SHA256}DyTmsEksfJ6GyfoledJlve==  
orclpasswordoldid: 16AC7/MSA-PN1iW6wXV1X27-1B4d6eG0G0A==
```

## 데일리시큐

카스퍼스키, 다크웹서 230만개 은행 카드 유출 확인...인포스틸러 위험↑

HOME > 이슈 > 주의

## 카스퍼스키, 다크웹서 230만개 은행 카드 유출 확인...인포스틸러 위험↑

윤 길만권 기자 | © 승인 2025.03.12 09:13

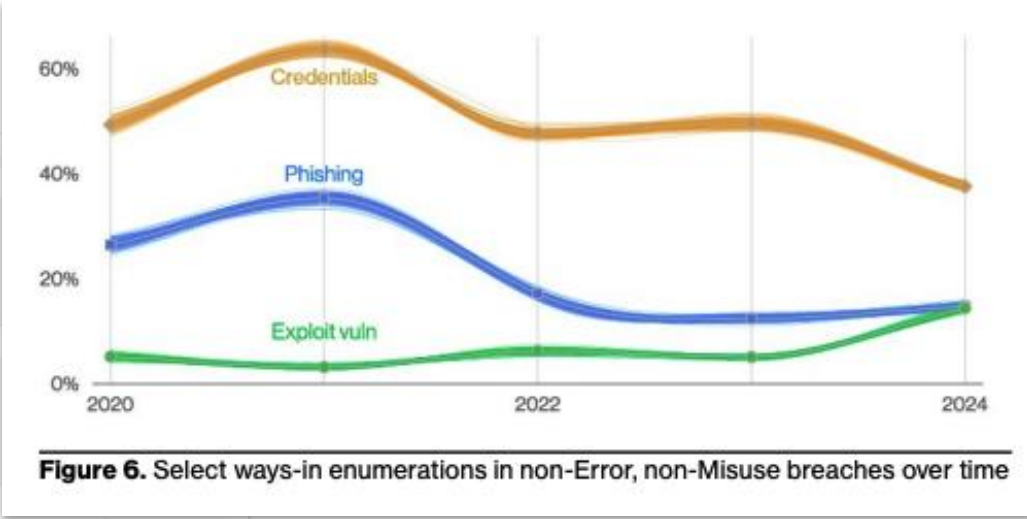
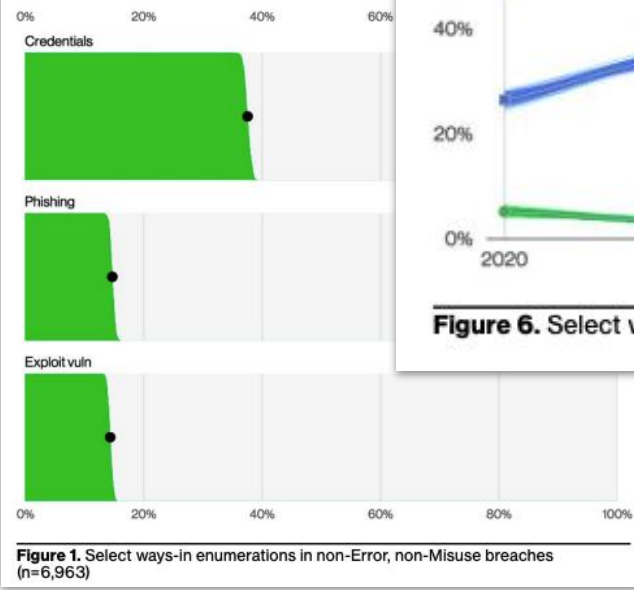


가장 위험적인 인포스틸러 악성코드...레드라인, 라이즈프로, 스틸크  
윈도우 OS 사용하는 기기 중 약 2,600만 대, 인포스틸러 악성코드에 감염

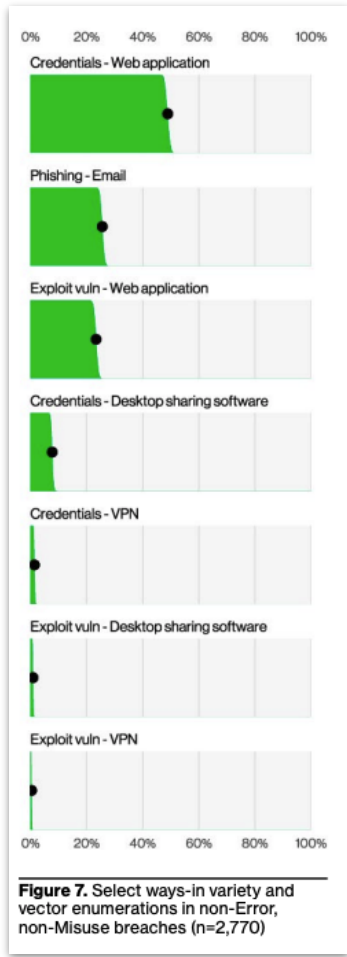


# 계정유출(Credential Leaks)

# 계정유출의 위험



출처: Verizon Data breach Investigation 2024





# 침투용 계정 거래 현황(다크웹)

Crasty\_bro라는 랜섬웨어 및 초기 네트워크 접근 계정 공급책은 stealer log에서 VPN, RDP, Citrix 접근 계정 등을 찾아 공급함(잘 알려진 로그인 URL)

<b>Crasty_bro</b> Premium	PowerGrep
Premium	
registration: 25.01.2021	TOTAL format : 6023 matches in 2630 files
Posts: 36	vpn / index.html
Reactions: 1	/vpn/tminindex.html
	/ citrix /
	RDWeb
	/ global-protect / login

XSS forum post, Networks sold by Crasty\_bro

07/20/2021 - [crasty_bro] Selling RDWeb Access to Supreme Foodservice - USA - \$1600
06/05/2021 - [crasty_bro] Selling Access to EG Group - UK - \$1800
06/09/2021 - [crasty_bro] Selling ManageEngine Access to MSP Outscope - Portugal - \$1000
06/10/2021 - [crasty_bro] Selling Citrix StoreFront Access to Luz del Sur - Peru - \$900
07/20/2021 - [crasty_bro] Selling Access to Trex - Turkey - \$600
07/21/2021 - [crasty_bro] Selling VMWare Horizon Access to Scheppers Wetteren - Belgium - \$900
04/30/2021 - [crasty_bro] Selling RDWeb Access to UK Halifax Academy and Washington University, St. Lc
08/25/2021 - [crasty_bro] Selling RDWeb Access to STG-HealthCare - USA - \$2500
07/21/2021 - [crasty_bro] Selling PulseVPN Access to Basilicata - Italy - \$800
07/21/2021 - [crasty_bro] - Selling Citrix Access to HSB - Sweden - \$700
05/23/2021 - [crasty_bro] Selling Access to Multiple Entities - \$10,000
07/20/2021 - [crasty_bro] Selling RDWeb Access to Bedford Group - AU - \$1500

# 사례A:고객정보 판매 게시(다크웹)

고객정보 유출  
(해킹)

다크웹에 “고객정보  
팝니다” 게시

다크웹에서 거래  
완료

현금화  
시도



# 사례A:고객정보 판매 게시(다크웹)

Customer: 849,960 full information  
USD:2,000

## SendGrid Twilio Database

Posted in BreachForums 2

Posts in thread 8

First posting Apr 3, 2025, 14:30

Most recent posting Apr 5, 2025, 20:15

Previous 10 Next 10

Hello BreachForums,

We would like to announce the breach of the largest Email Hosting Provider - **SendGrid** is cloud-based email infrastructure provider businesses with email delivery management.

( 3 April 2025 )

>>Wikipedia Page<<

+ Company General:

Quote:

**SendGrid** (also known as **Twilio SendGrid**)

**SendGrid** provides a cloud-based service that assists businesses with email delivery.

[7][9][20][21] The service manages various types of email including shipping notifications, friend requests, sign-up confirmations, and email newsletters.

It also handles **Internet service provider (ISP)** monitoring, domain keys, the **sender policy framework (SPF)**, and feedback loops.

[13][22][23][24] Additionally, the company provides link tracking and open rate reporting.

[22] It also allows companies to track email opens, unsubscribes, bounces, and spam reports.

[7][22][25] Beginning in 2012, the company integrated SMS, voice, and push notification abilities into its service through a partnership with **Twilio**.

[15]

We're Selling **Twilio SendGrid** Database:

→ <https://sendgrid.com>

Database Includes:

+ 848,960 Customers full informations "Emails,Phone Numbers,Address,City,State,Country,Social Media,LinkedIn\_ID...much more".

+ 848,960 Companies full informations "Page Rank,CIK No,SIC Code,Sales Revenue,Employees,SEO,Domain Names,Cloudflare Rank,Hosting Provider,Revenue,Operating Income,Net Income... much more".

+ Employees Details.

+ Companies Net-worth, Income, Performance...

Much More...

Sample: <https://www.upload.ee/files/17927288/sen...e.csv.html>

Full Database Price: \$2,000

Telegram: (Dark X) @darkthemr666

## SendGrid Twilio Database

Posted in BreachForums 2

Posts in thread 8

First posting Apr 3, 2025, 14:30

Most recent posting Apr 5, 2025, 20:15

Previous 10 Next 10

Just read an article about this.

**Twilio** rejected the entire thing saying none of the platforms were breached.

Post 3 of 8 by Crockett on Apr 4, 2025, 02:37

Good Day!

Here's a bigger sample ( 10,000 lines ) : <https://www.upload.ee/files/17929309/part10k.csv.html>

Post 4 of 8 by Satanic on Apr 4, 2025, 05:22

it seem Twilio say after checking the data sample it not associate with **sendgrid**, but it hard to confirm if they are telling the truth or lying.

Post 5 of 8 by nyep on Apr 4, 2025, 09:29

(37 minutes ago)

nyep Wrote:

it seem Twilio say after checking the data sample it not associate with **sendgrid**, but it hard to confirm if they are telling the truth or lying.

They said the database wasn't taken directly from **SendGrid**'s servers.

My response was to send them a massive sample to double-check.

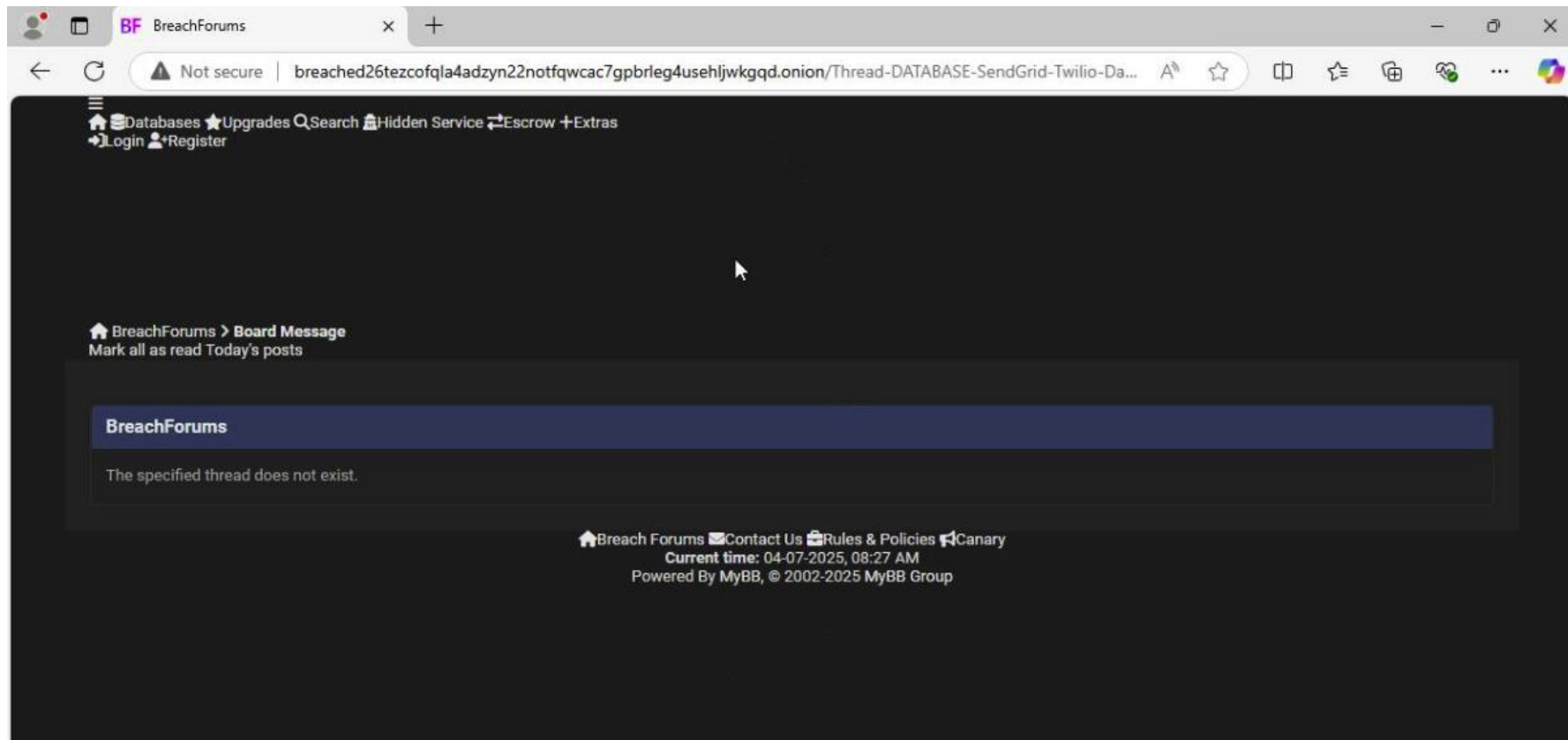
Whatever, i'm not looking for confirmation of anybody since the data is legit.

It is not in my best interest to share the source and how it was hacked.

Post 6 of 8 by Satanic on Apr 4, 2025, 10:03



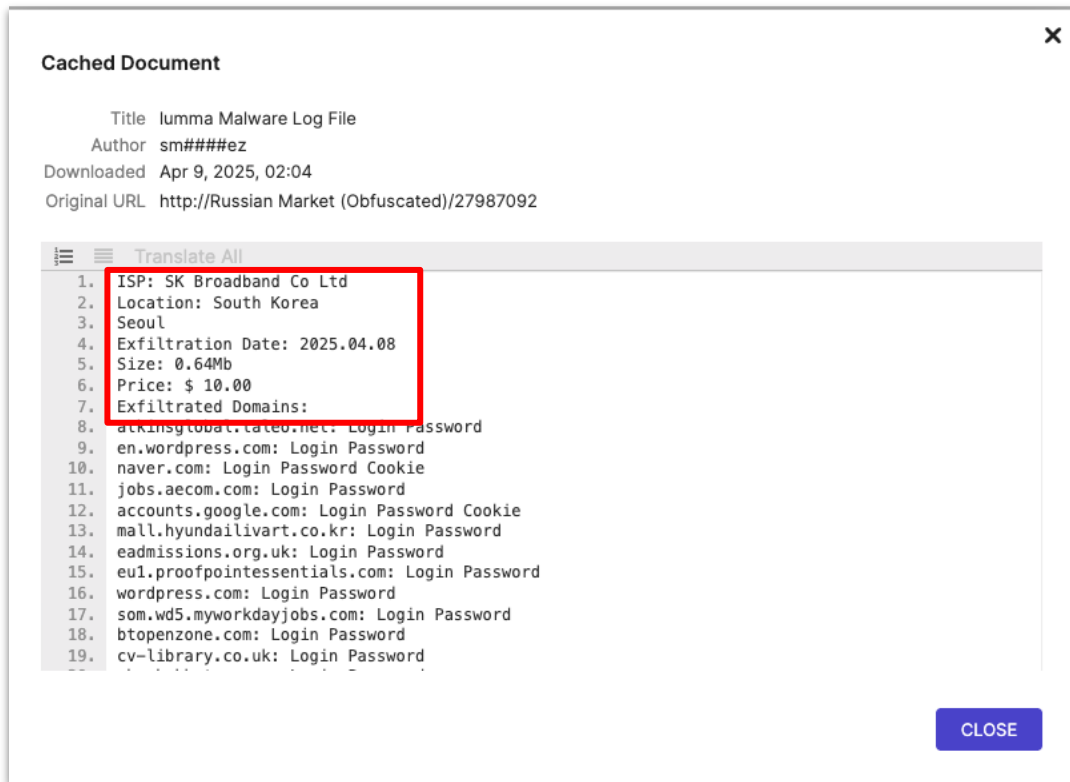
# 사례A:고객정보 판매 게시(다크웹)



# 사례B:domain login 자격증명 판매 게시(다크웹)

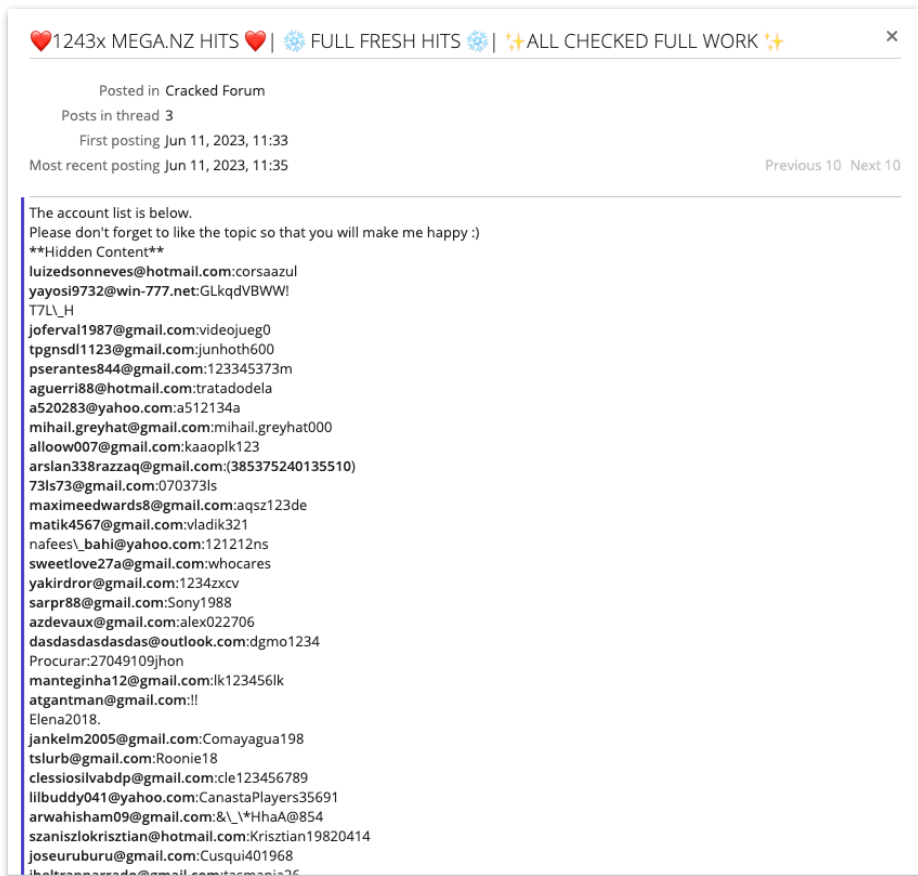


# 사례B:domain login 자격증명 판매 게시(다크웹)



USD10  
975 domain  
password/cookie

# 다크웹 덤프의 경우는 ID/Password 제공



다크웹에 유출된 형태,  
단순 ID:PWD 을 제공함. 어디에 사용되는 계정인지는  
제공하지 않음(credential stuffing 공격으로 활용)  
피싱공격으로도 많이 활용됨



# Stealer Malware

## 왜 위험한가?

# 사례B:domain login 자격증명 판매 게시(다크웹)

InfoStealer감염  
(해킹)

다크웹에 "로그인계정  
판매글" 또는 덤프

다크웹에서 거래  
완료

구매계정으로 침투

해킹  
(고객정보/파괴 등등)



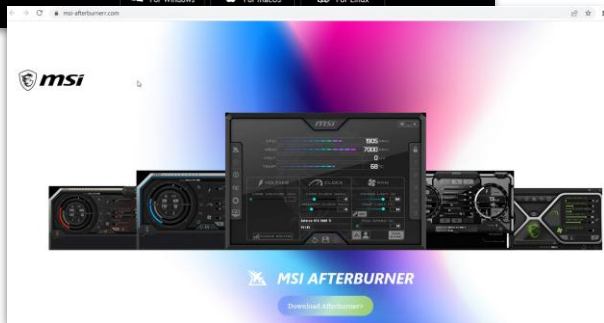
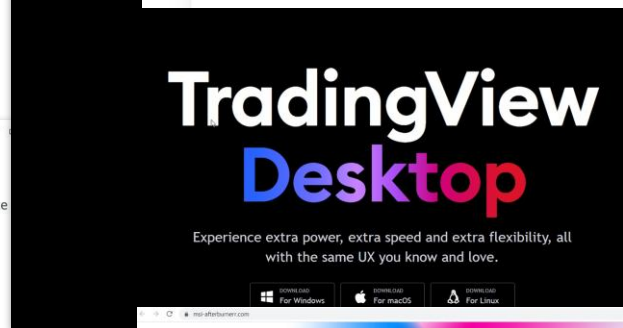
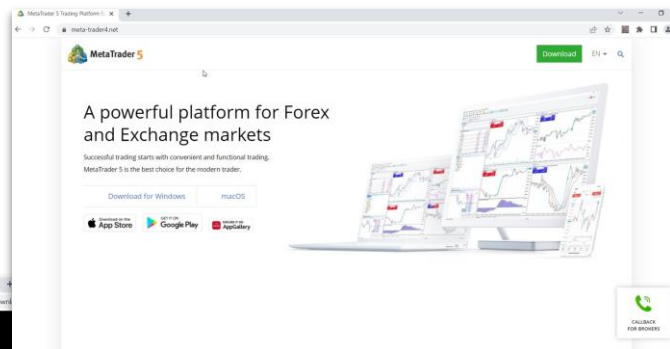
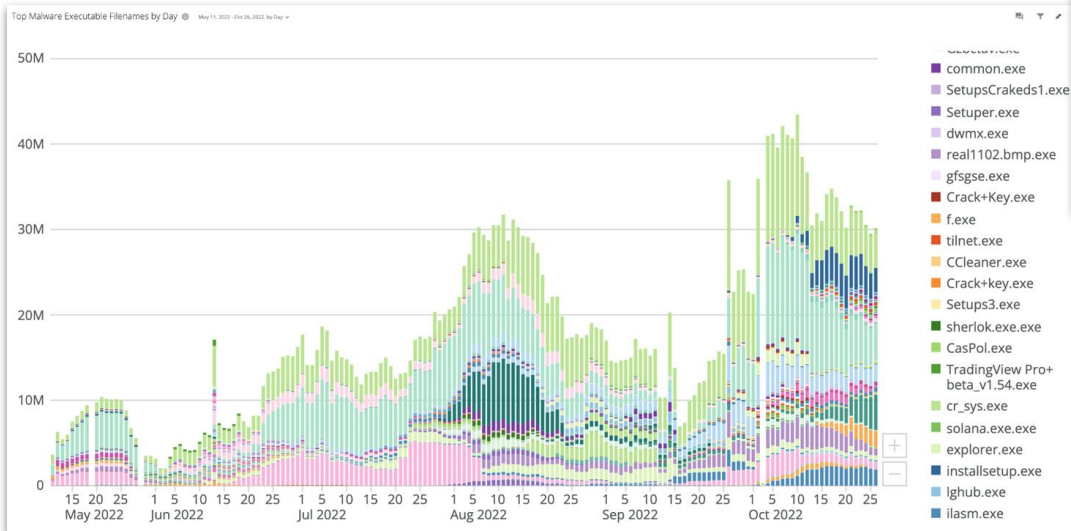
CTI벤더 탐지

침해사고 대응



# Stealer 악성코드 감염경로

불법 소프트웨어 다운로드 금지!



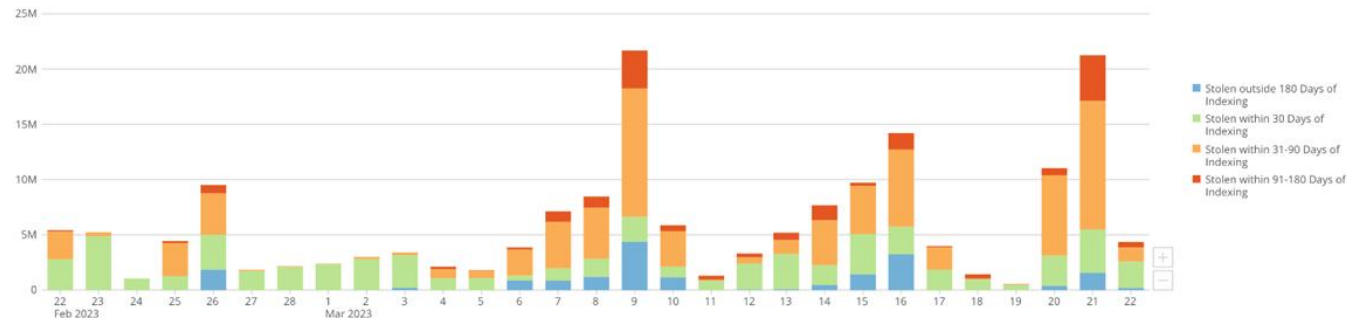
# InfoStealer Malware 예제

abahgamers21@gmail.com	Jun 14, 2023	https://ftx.com/trade/TRX/USDT
Name	Stealer Malware Logs 2023-06-11	
Identity	abahgamers21@gmail.com	
Domain	ftx.com	
Authorization URL	https://ftx.com/trade/TRX/USDT	
Description	This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.	
Detection Date	Jun 14, 2023, 03:28	
Exfiltration Date	Jun 12, 2023, 07:08	
Type	Clear	
Hashes	Algorithm: SHA1	Hash: 572bef0a27a3e3e252289d6178c8ab0ccb4b23e4
	Algorithm: SHA256	Hash: e729c85ac05e9beb7a2e73334aa9484ef86538651fe40ec59742047c2651ad46
	Algorithm: NTLM	Hash: 782729f0658c880a03b2bc2b6388f479
	Algorithm: MD5	Hash: a840a753493d953bc3edb5ef7fbed6ea
Properties	Letter, Number, Symbol, UpperCase, LowerCase, AtLeast12Characters	
Password	Ba*****	
Effectively Clear	True	
Malware Family	Meta Stealer	
Compromised Host	Operating System: Windows 10 Enterprise x64	
	OS User Name: BR	
	File Path Location: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe	
	Time Zone: UTC+07:00	
	Name of the Machine: N/A	
	User Account Control Setting: N/A	
	Antivirus: Windows Defender	

- 유출계정
- 로그인 계정 target URL
- 유출날짜
- 비밀번호(cleartext로 유출됨), 플랫폼에서는 앞2자리만 힌트로 제공
- Meta Stealer 악성코드 위치

# 악성코드에 의해 유출되는 계정(ID:PWD:Auth domain)

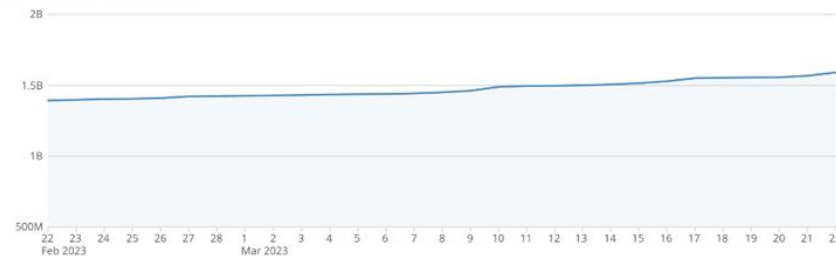
Credential Exfiltration Freshness for Last 30 Days



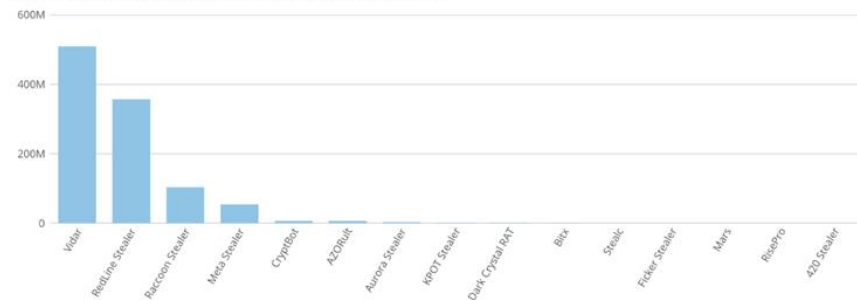
Freshness in this context refers how recently the credentials were exfiltrated (collected via malware) relative to the index date (when we process it). We can see that most of our recently indexed credentials were stolen in last 30 days, indicating we are processing good data and adding value for the customer.

Malware Credentials Running Total Last 30 Days by Day

203M Creds Indexed Last 30 Days



Total Malware Credentials Indexed by Family All-Time



Dark web Dump vs. Stealer

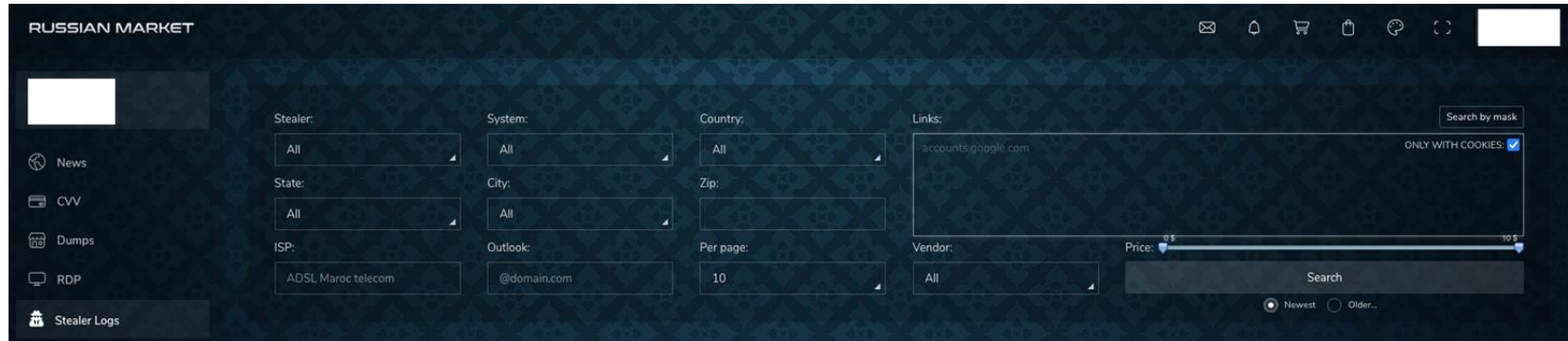
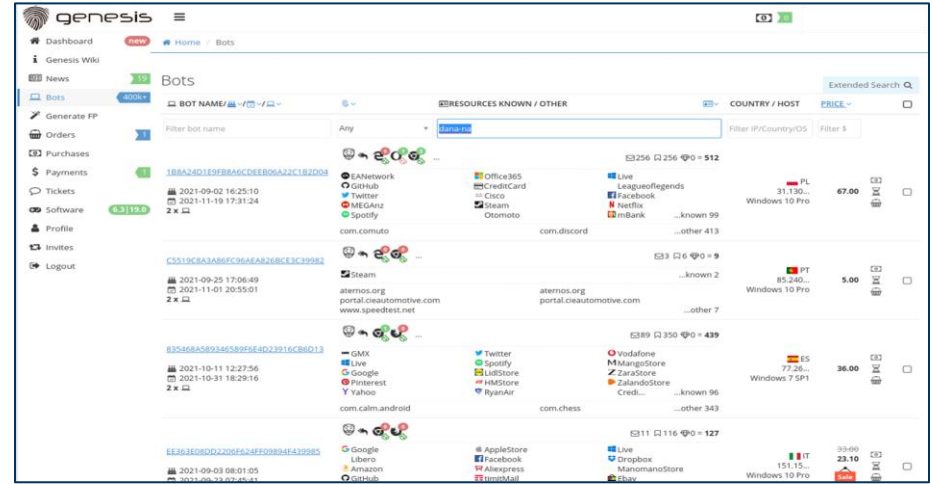


# Darkweb Market

# 다크웹 암시장(Dark Web Markets)

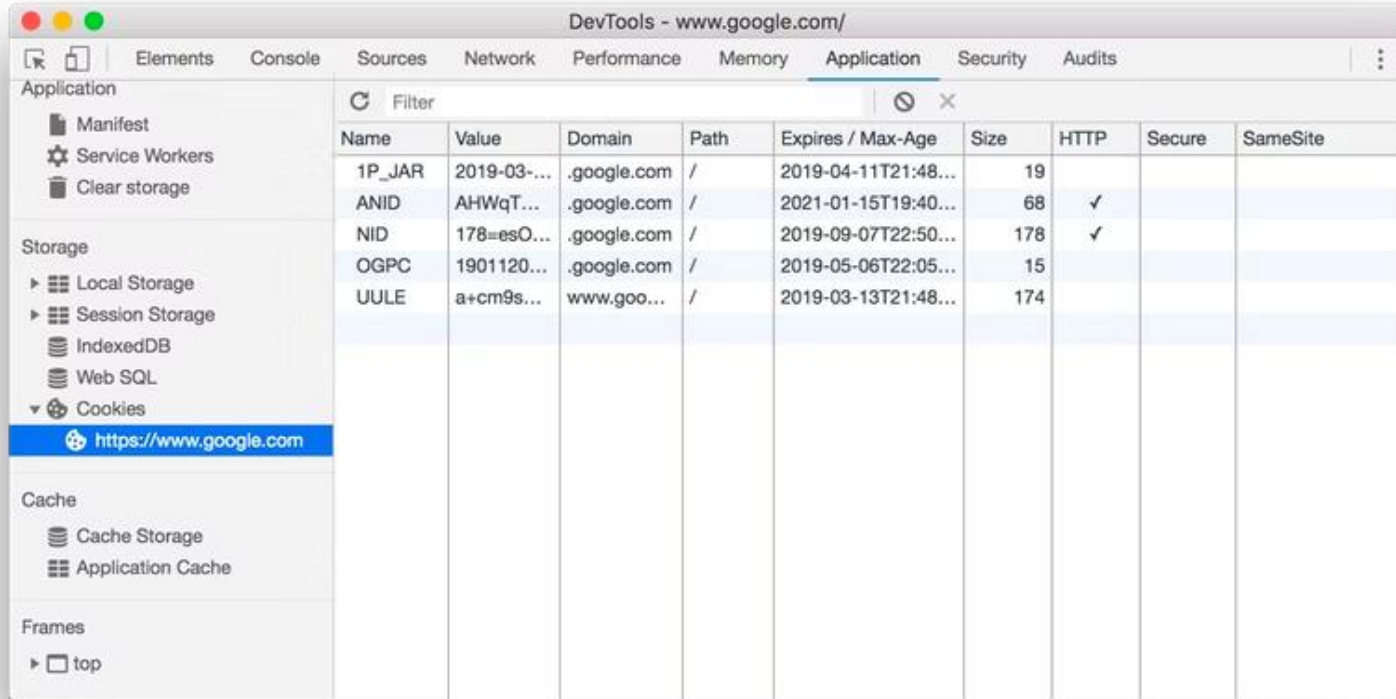
Genesis 암시장은 계정판매 전문 사이트:

- FingerPrints (FP),
- Cookies,
- Inject Scripts info,
- Form Grabbers (Logs),
- Saved Logins,
- Other personal data



# Cookie-based Authentication

## Google Chrome Developer Tools



The screenshot shows the Google Chrome Developer Tools interface with the 'Application' tab selected. The left sidebar shows the 'Storage' section expanded, with 'Cookies' selected. The main pane displays a table of cookies for the domain 'www.google.com'.

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
1P_JAR	2019-03-...	.google.com	/	2019-04-11T21:48...	19			
ANID	AHWqT...	.google.com	/	2021-01-15T19:40...	68	✓		
NID	178=esO...	.google.com	/	2019-09-07T22:50...	178	✓		
OGPC	1901120...	.google.com	/	2019-05-06T22:05...	15			
UULE	a+cm9s...	www.goo...	/	2019-03-13T21:48...	174			



# Importing Cookies

Proxy (socks5)

180.197.86.236

7391

Save Proxy

Clear Proxy ✕

Current Browser data

Bot:	46571A87-E544B574-4FDF9573-F022EE62-CFE0106A
Browser:	chrome (Chrome 72.0.3626.121)
Cookies:	3139
History:	0
Memory Used:	1 Mb

Get CookiesPut Cookies

Bots & Fingerprints

46571A87-E544B574-4FDF9573-F022EE62-CFE0106A (chrome)

chrome , cookies 3141 , fingerprints 1

Select Fingerprint

Get New Bots

Import Cookies

Install & Save FP Settings

☒ Ignore expire Date

☐ Use Current Proxy IP for WebRTC

Remove Bot ✕

Remove Browser ✕

Remove FP ✕

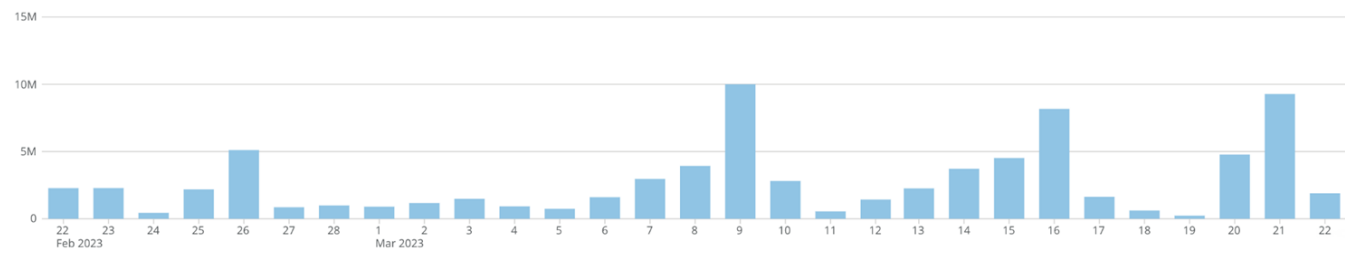
# Credentials with Cookies

유출된 계정의 40%는 쿠키를 포함하고 있음

Malware Creds with Cookies Last 30 Days

by Day

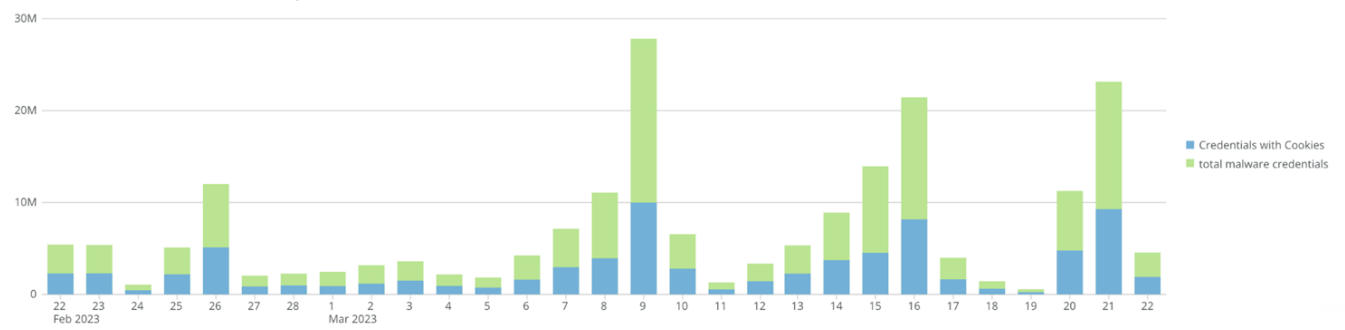
80M Credentials with Cookies Indexed in Last 30 Days



Malware Creds with Cookies as a Portion of Totals Creds Last 30 Days

by Day


80M Credentials with Cookies Indexed in Last 30 Days



# Automated Browser Fingerprinting

← → ↻ 🏠 🔒 https://genesis.market/client/client-purchases/index ☆ 🧑🏻 0 👤 ⋮

📱 Apps 📄 Iron Forum 📄 Iron for Android 📄 Iron Extensions

 ☰

👁 6 💰 320.00 👤 client ▾

[🏠 Dashboard](#) [🏠 Home](#) / [Client Purchases](#)

[📰 News](#) 6

[💻 Bots](#) 65694

[🔧 Generate FP](#) new

[🛒 Orders](#)

[💰 Purchases](#) 6

[💵 Payments](#)

[💬 Tickets](#)

[🛡 Genesis Security](#)

[👤 Profile](#) 4.5.1

[👤 Invites](#)

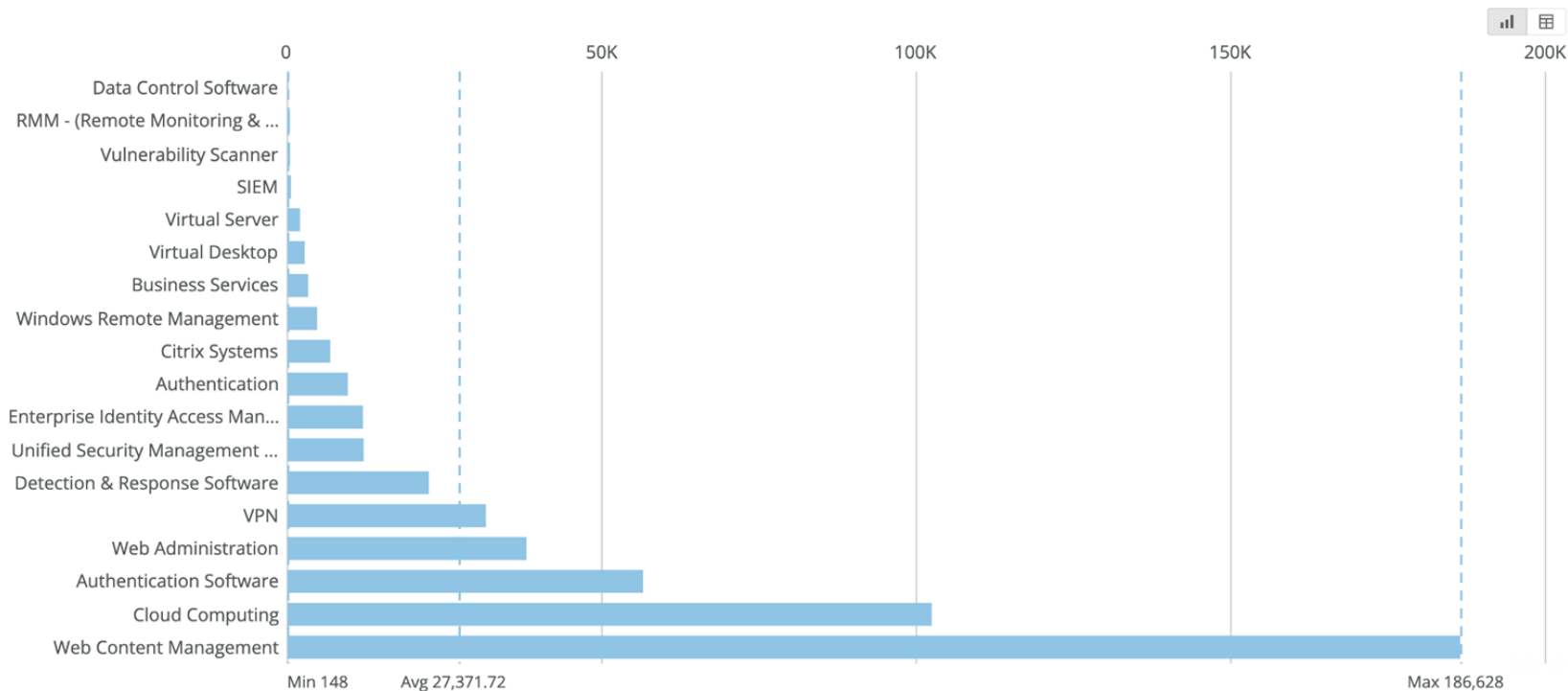
[🚪 Logout](#)

## Client Purchases

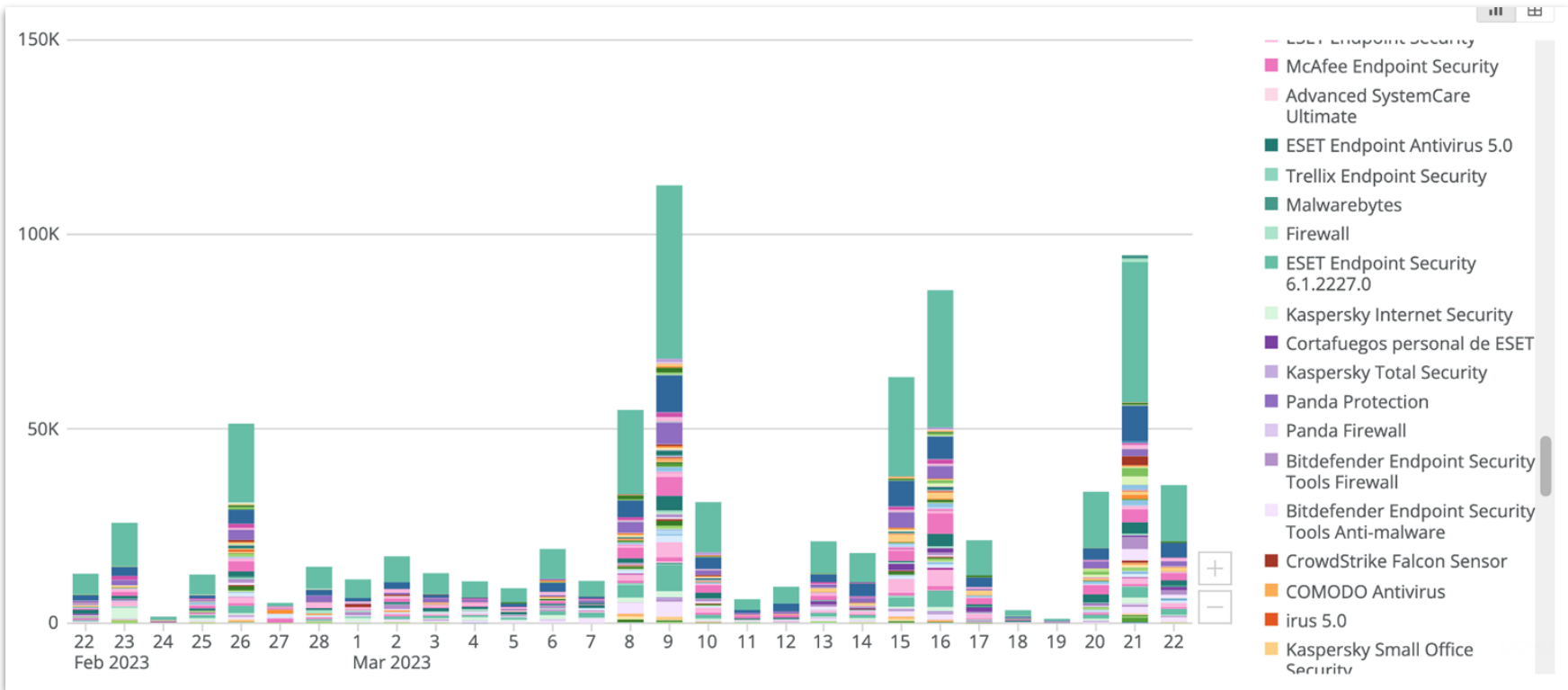
BOT NAME/📅/📅 ▾	<a href="#">SORT FP</a> 🧑🏻 ▾	📄 RESOURCES KNOWN / OTHER	<a href="#">SORT</a> 📄 ▾	COUNTRY / HOST	<a href="#">PRICE</a> ▾
Any ▾	Any ▾	Filter resource name/domain: paypal,ebay.com,hotmail.com...		Filter IP/Country/OS	Filter \$
📅 11/03/2019 12:15:02 <b>Purchased</b>	🧑🏻 ↻ 🧑🏻 1		📧 0 📄 9 💎 0 = 9		
<a href="#">PC1-VAIO_4558adb2cb76befd54a8</a>	Facebook	...known 4		🇪🇸 ES 95.19.6.38	8.00
📅 2018-01-25 01:06:26 📅 2018-02-11 21:31:00 <b>viewed</b>	www.foroexplayate.com www.trabajos.com	www.bbva.es ...other 5			
📅 11/03/2019 12:11:33 <b>Purchased</b>	🧑🏻 ↻ 🧑🏻 0 🧑🏻 0		📧 0 📄 4 💎 0 = 4		
<a href="#">08CE77D0-E544B574-A12EE511-6607AD56-A6DD888F</a>				🇵🇹 PT 109.48.208.5	2.00

# 영향 받는 제품군들

계정은 단순히 개인의 소셜계정 크레덴셜 유출이 아니라, 기업의 침투용으로 사용

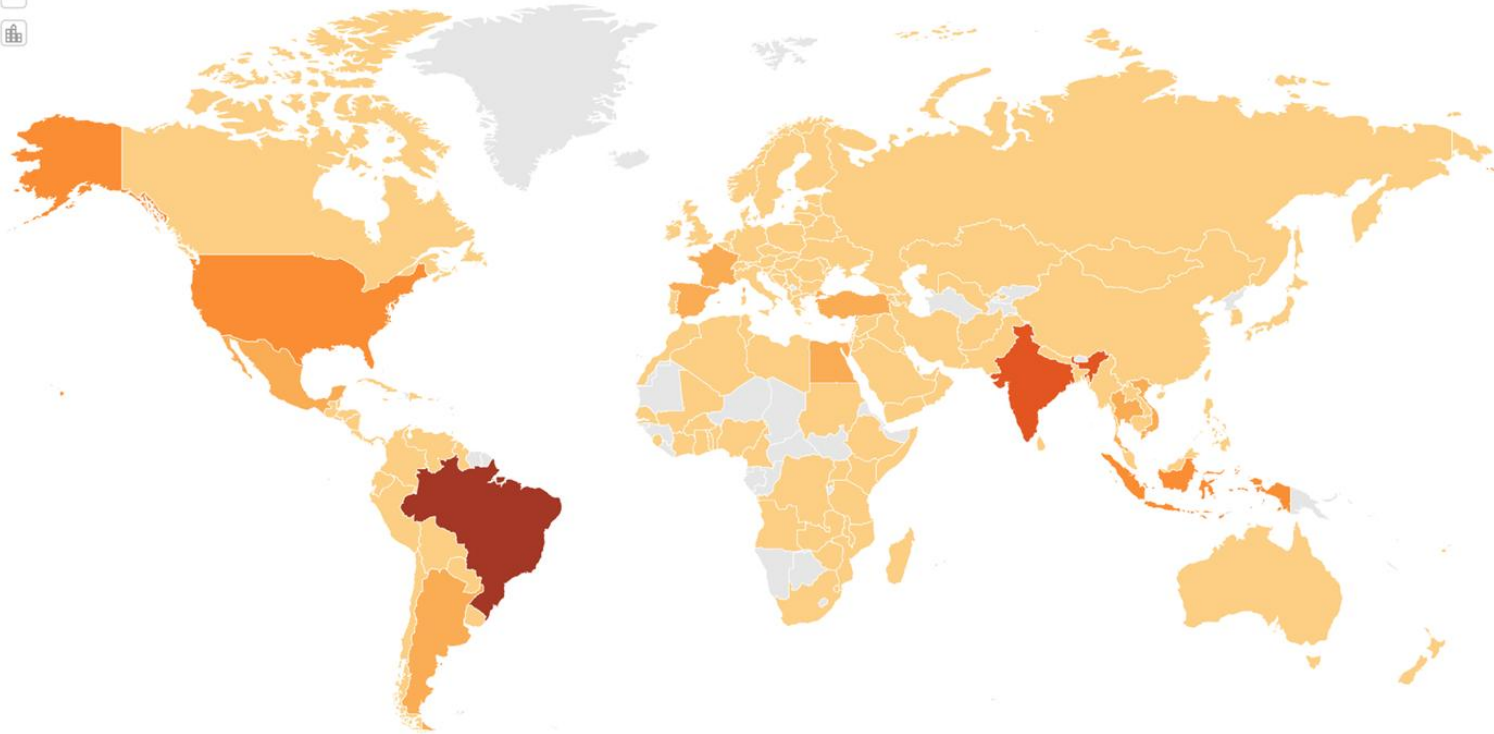


# 개인용/기업용 백신도 탐지 우회



Windows/McOS 모두 Stealer Malware에 취약함

# 글로벌 이슈



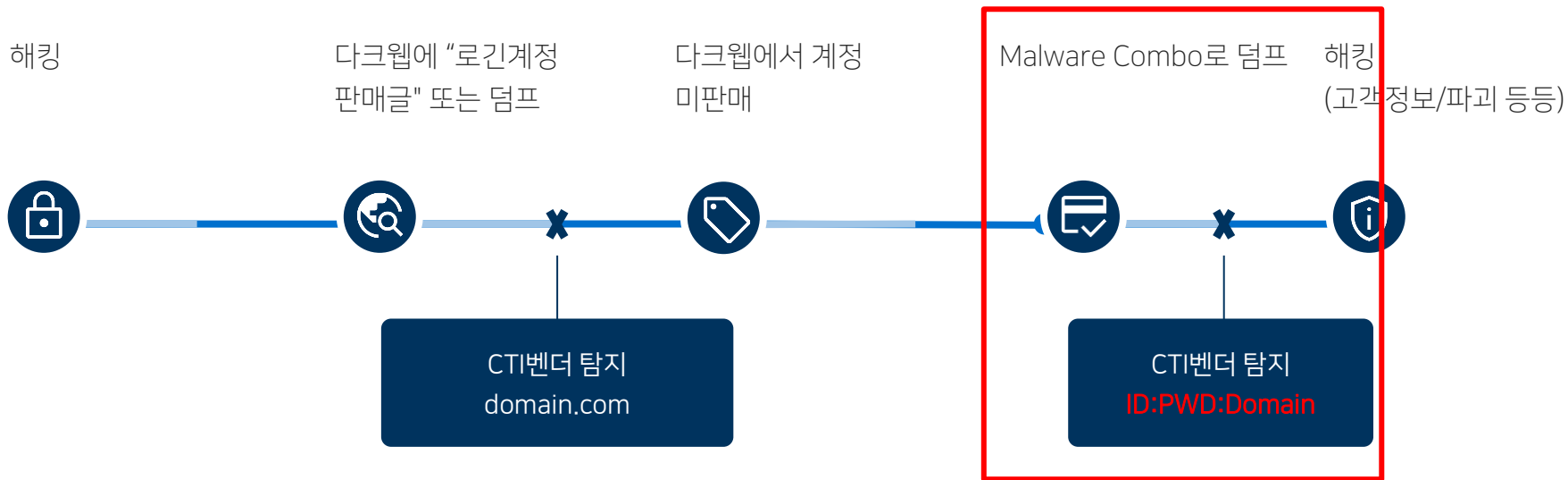




# 새로운 Dump (Malware Combo)

# Malware Combo Dump

로그인 계정 미판매분만 공개되는지는 알 수 없음



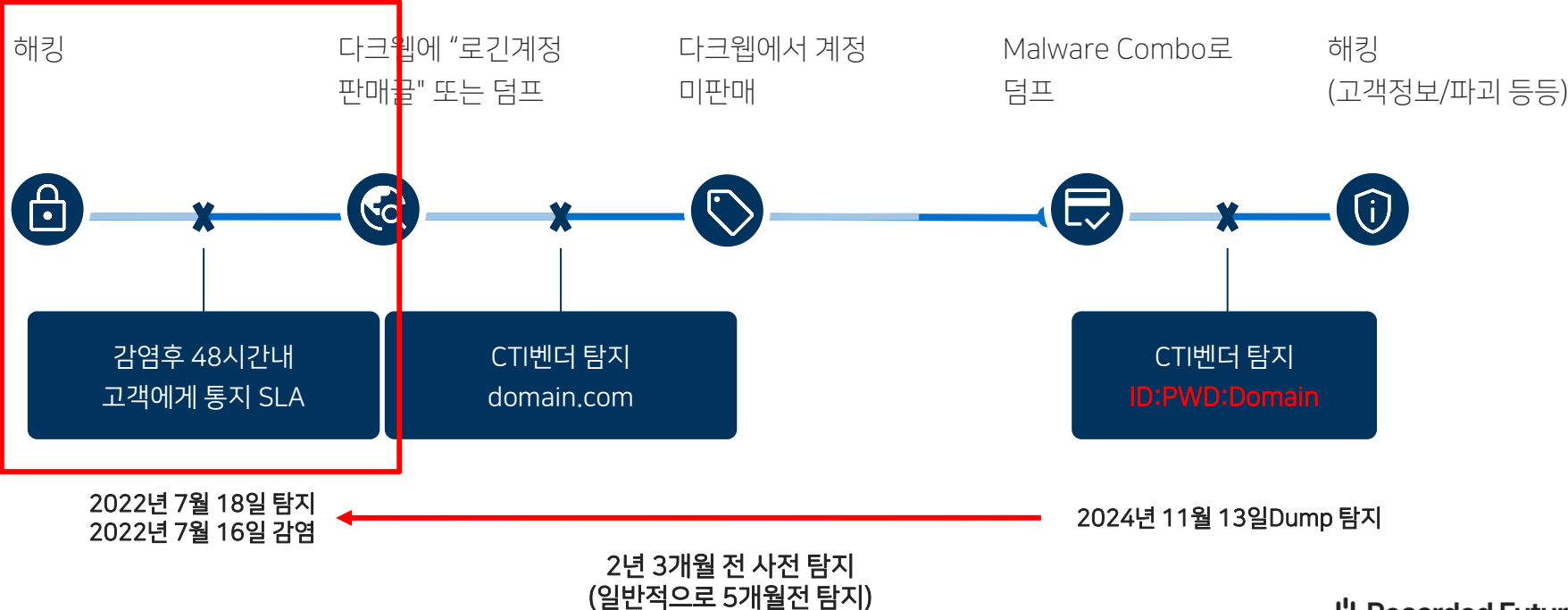
# Malware Combo Dump 예제

## ID/Password/Domain 정보 제공

Exposure 1	
Name	Malware Combo Lists
Identity	seongm [redacted]
Domain	edumadang.s [redacted]
Authorization URL	https://edumadang [redacted] /index.php
Description	Malware Combo Lists is a collection of credentials from various combo lists that were shared publicly or privately on the dark web. Due to the nature of combo lists, these types of sources do not come with a specific connection to any one site, and will often be recycled from other sources. There is no associated breach record for this source.
Last Downloaded Date	Nov 13, 2024, 10:12
Exfiltration Date	-
Type	Clear
Hashes	Algorithm: SHA1      Hash: 4c1e
	Algorithm: SHA256      Hash: bef5
	Algorithm: NTLM      Hash: 7e12
	Algorithm: MD5      Hash: d183
Properties	Letter, Number, Symbol, LowerCase, AtLeast10Characters
Password	ch.... ⓘ
Compromised Host	Operating System: N/A
	OS User Name: N/A

# Intelligence-Led Security

스틸러에 의해 유출 된 정보가 다크웹마켓에 게시/combo dump 이전에 사전탐지후 경고발생



# RedLine Stealer 탐지

2022년 7월 16일

Exposure 1 2	
Name	Stealer Malware Logs 2022-07-16
Identity	seongn[REDACTED]
Domain	edumadang[REDACTED]
Authorization URL	https://edumadang[REDACTED]/index.php
Description	This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.
Last Downloaded Date	Jul 18, 2022, 21:30
Exfiltration Date	Jul 16, 2022, 22:09
Type	Clear
Hashes	Algorithm: SHA1 Hash: 4c1e
	Algorithm: SHA256 Hash: bef5
	Algorithm: NTLM Hash: 7e12
	Algorithm: MD5 Hash: d183
Properties	Letter, Number, Symbol, LowerCase, AtLeast10Characters
Password	ch**** ⓘ
Compromised Host	Operating System: Windows 10 Enterprise x64
	OS User Name: mio12
	File Path Location: UNKNOWN
	Time Zone: UTC+09:00
	Name of the Machine: N/A
	User Account Control Setting: AllowAll
Malware Family	Antivirus: Windows Defender
	RedLine Stealer MALWARE
	Technology
	Category: N/A
	Tag: N/A
	IP Address
Country	218.239.224.61
	Korea (the Republic of)
	Postal Code
Antivirus	44236

# RedLine Stealer 탐지

피해자 IP를 조회 결과, 총 157개 domain 계정 유출

157 Results for 218.239.224.61

Exposure 1 2

Name	Stealer Malware Logs 2022-07-16	
Identity	admin	
Domain	192.168.33.1	
Authorization URL	http://192.168.33.1/session/login_session.cgi	
Description	This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.	
Last Downloaded Date	Jul 18, 2022, 21:30	
Exfiltration Date	Jul 16, 2022, 22:09	
Type	Clear	
Hashes	Algorithm: SHA1	Hash: d033e22ae348aeb5660fc2140aec35850c4da997
	Algorithm: SHA256	Hash: 8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
	Algorithm: NTLM	Hash: 209c6174da490caeb422f3fa5a7ae634
	Algorithm: MD5	Hash: 21232f297a57a5a743894a0e4a801fc3
Properties	Letter, LowerCase	
Password	ad**** ⓘ	
Compromised Host	Operating System: Windows 10 Enterprise x64	
	OS User Name: mio12	
	File Path Location: UNKNOWN	
	Time Zone: UTC+09:00	
	Name of the Machine: N/A	
	User Account Control Settings: AllowAll	





Stealer > Malware combo > dump  
기 유출된 credential은 더이상 사용금지  
Security Awareness Training

# 우리 회사 계정 유출 보고서 받아보기(무료)

<https://www.recordedfuture.com/ko/products/identity-intelligence>

Recorded Future®

플랫폼 결과 제품 서비스 리서치 리소스 회사 🔍

데모 받기

## Request a Complimentary Report of Your Organization's Credential Exposures

77% of web application breaches begin with stolen credentials<sup>1</sup> with identity as the primary attack vector for modern threat actors. Our complimentary Identity Exposure Assessment reveals credential exposure data specific to your organization's domain.

Access your report here



Recorded Future®

# 질의 응답?

