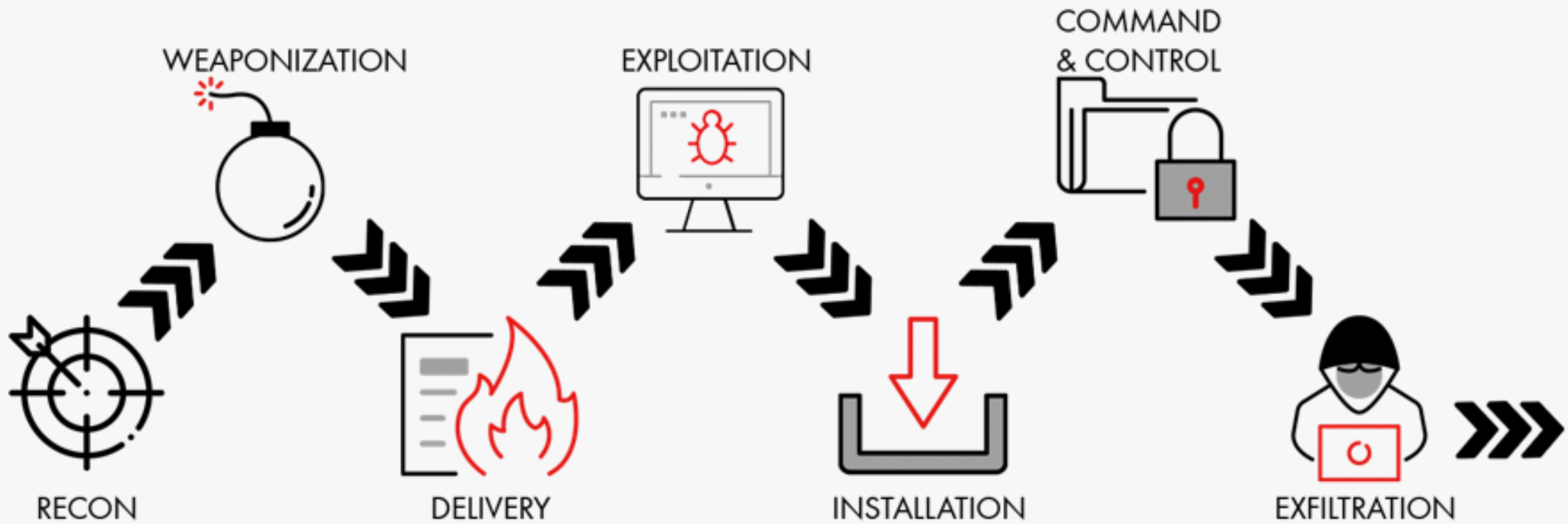




**SATAYO is on fire!**

# Coverage of the recon phase

Schema Lockheed Martin Cyber Kill Chain





# 2022 DEVELOPMENT ROADMAP

**satay**

#WEINNOVATE

Last Update	URL	STATUS	#
2022-10-24 01:00:58	<a href="#">Our DB</a>	Our DB	2
2022-10-24 01:00:58	<a href="https://raw.githubusercontent.com/Orange-Cyberdefense/russia-ukraine_IOCs/main/OCD-Datalake-russia-ukraine_IOCs-ALL.csv">https://raw.githubusercontent.com/Orange-Cyberdefense/russia-ukraine_IOCs/main/OCD-Datalake-russia-ukraine_IOCs-ALL.csv</a>	200	7802
2022-10-24 01:00:58	<a href="https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt">https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt</a>	200	71226
2022-10-24 01:00:57	<a href="https://phishing.army/download/phishing_army_blocklist_extended.txt">https://phishing.army/download/phishing_army_blocklist_extended.txt</a>	200	159090
2022-10-24 01:00:56	<a href="https://phishing.army/download/phishing_army_blocklist.txt">https://phishing.army/download/phishing_army_blocklist.txt</a>	200	155967
2022-10-24 01:00:54	<a href="https://blocklist.cyberthreatcoalition.org/vetted/domain.txt">https://blocklist.cyberthreatcoalition.org/vetted/domain.txt</a>	Unable to establish a connection.	0
2022-10-24 01:00:33	<a href="https://zerodot1.gitlab.io/CoinBlockerLists/list.txt">https://zerodot1.gitlab.io/CoinBlockerLists/list.txt</a>	200	276183
2022-10-24 01:00:30	<a href="https://www.botvrij.eu/data/ioclist.hostname.raw">https://www.botvrij.eu/data/ioclist.hostname.raw</a>	200	93
2022-10-24 01:00:29	<a href="https://feeds.alphasoc.net/ryuk.txt">https://feeds.alphasoc.net/ryuk.txt</a>	404	0
2022-10-24 01:00:29	<a href="https://gist.githubusercontent.com/BBcan177/4a8bf37c131be4803cb2/raw">https://gist.githubusercontent.com/BBcan177/4a8bf37c131be4803cb2/raw</a>	200	17313
2022-10-24 01:00:29	<a href="https://www.botvrij.eu/data/ioclist.domain.raw">https://www.botvrij.eu/data/ioclist.domain.raw</a>	200	123
2022-10-24 01:00:25	<a href="https://api.abuseipdb.com/api/v2/blacklist">https://api.abuseipdb.com/api/v2/blacklist</a>	200	100000
2022-10-24 01:00:21	<a href="https://www.dan.me.uk/torlist/">https://www.dan.me.uk/torlist/</a>	403	0
2022-10-24 01:00:14	<a href="http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt">http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt</a>	200	52900
2022-10-24 01:00:14	<a href="http://www.ipspamlist.com/public_feeds.csv">http://www.ipspamlist.com/public_feeds.csv</a>	200	6
2022-10-24 01:00:14	<a href="https://sslbl.abuse.ch/blacklist/sslipblacklist.csv">https://sslbl.abuse.ch/blacklist/sslipblacklist.csv</a>	200	36
2022-10-24 01:00:14	<a href="https://raw.githubusercontent.com/LinuxTracker/Blocklists/master/HancitorIPs.txt">https://raw.githubusercontent.com/LinuxTracker/Blocklists/master/HancitorIPs.txt</a>	200	872
2022-10-24 01:00:14	<a href="http://blocklist.greensnow.co/greensnow.txt">http://blocklist.greensnow.co/greensnow.txt</a>	200	5035
2022-10-24 01:00:14	<a href="https://feodotracker.abuse.ch/downloads/ipblocklist.csv">https://feodotracker.abuse.ch/downloads/ipblocklist.csv</a>	200	478
2022-10-24 01:00:13	<a href="http://www.darklist.de/raw.php">http://www.darklist.de/raw.php</a>	200	6040
2022-10-24 01:00:10	<a href="https://rules.emergingthreats.net/blockrules/compromised-ips.txt">https://rules.emergingthreats.net/blockrules/compromised-ips.txt</a>	200	875
2022-10-24 01:00:07	<a href="http://cinsscore.com/list/ci-badguys.txt">http://cinsscore.com/list/ci-badguys.txt</a>	200	15000
2022-10-24 01:00:04	<a href="https://www.botvrij.eu/data/ioclist.ip-dst.raw">https://www.botvrij.eu/data/ioclist.ip-dst.raw</a>	200	99
2022-10-24 01:00:04	<a href="https://lists.blocklist.de/lists/all.txt">https://lists.blocklist.de/lists/all.txt</a>	200	20792
2022-10-24 01:00:01	<a href="http://reputation.alienvault.com/reputation.data">http://reputation.alienvault.com/reputation.data</a>	200	609
2022-10-24 01:00:01	<a href="https://gist.githubusercontent.com/BBcan177/bf29d47ea04391cb3eb0/raw/">https://gist.githubusercontent.com/BBcan177/bf29d47ea04391cb3eb0/raw/</a>	200	3074

# SATAYO IoC

### Admin Breach

Discover the attack surface, keep it monitored, and manage the exposed data over time. React proactively in order to avoid exploits.  
(admin)

SEC4U: 27,307,593,488  
TOT: 31,503,792,438

Rows: 1-200 / 652 Page 1 of 4 Records: 200

Logo	Date	Name		568 empty	568 empty	583 empty	Mail	Comment	SEC4U
				3=widespread 2=on average widespread 1=not widespread	3=very critical data 2=average critical data 1=uncritical data	3=no element of complexity [ex. plaintext password] 2=medium level complexity elements [ex. hash] 1=high elements of complexity [ex. hash+salt]			
	2022-08-28	Wakanim - wakanim.tv		0	0	0	3		0
	2022-08-25	TAP Air Portugal - flytap.com		0	0	0	35		1
	2022-08-14	Brand New Tube - brandnewtube.com		0	0	0	0		0
	2022-08-08	Shitexpress - shitexpress.com		0	0	0	0		0
	2022-07-04	La Poste Mobile - lapostemobile.fr		0	0	0	0		0
	2022-05-21	QuestionPro - questionpro.com		0	0	0	38		0
	2022-05-16	Amart Furniture - amartfurniture.com.au		0	0	0	0		0
	2022-05-13	Mangatoon - mangatoon.mobi		0	0	0	0		0
	2022-05-04	BlackBerry Fans - blackberryfans.org		0	0	0	0		0
	2022-04-30	Fanpass - fanpass.co.uk		0	0	0	1		0

# Data breaches investment

- Among the top 3 platforms globally in terms of number of accounts
- Nearly 30 billion accounts, growing all the time
- Monitoring of sources as close as possible to the Threat Actor

MORE THAN SOFTWARE

## Status Managed

Discover the attack surface, keep it monitored, and manage the exposed data over time. React proactively in order to avoid exploits.

(admin)

## Active analysis for Würth IT

### Market

only potentially critical & critical resources

Severity	Stealer	Market	ID	Installed date	Updated date	Clean	Jira
	hotspot.wuerth-it.com	Genesis	94FE7DA6827AA7BDE91BF9EFFD473F24	2019-12-29 18:59:15	2019-12-29 23:53:39		
	hotspot.wuerth-it.com	Vidar	4390458	2022-07-24	2022-07-24		
	hotspot.wuerth-it.com	Racoon	4584997	2022-08-06	2022-08-06		
	fdv.wurth.fr	2easy	1595338634886701e8355d7a8e76bfd8b908b130ca	2020-07-21	2020-07-21		
	hotspot.wuerth-industrie.com hotspot.wuerth-industrie.com	Genesis	C2B2494F179E45271491C4E7E522207E	2022-09-22 16:21:45	2022-09-23 19:05:44		

### Deep Dark Web

ID research	Domain	URL	Title	Author	Content	Clean	Jira
4306	wuerth.de	https://searchcode.com/codesearch/view/17579611/	cambridge-pm-website - repo: git://github.com/bjdean/cambridge-pm-website.git /old-site/archive/2004-August/001094.html - lang: HTML - lines: 61		Armin Zendron <A HREF="mailto:armin.zendron@wuerth.it">armin.zendron@wuerth.it</A>		

### Domain Link


-(6 Month old)

ID research	Domain Link	Creation date	Domain	Jira
4317	urth.se	2022-08-29	wurth.se	

# Jira / Confluence integration

- The security analyst's job generates a ticket
- The client has the ability to interact with the ticket
- Communication speed (and remedy...)
- Measurable KPIs

# Jira / Confluence integration


JIRA
Your work ▾
Projects ▾
Filters ▾
Dashboards ▾
People ▾
Plans ▾
Assets
Apps ▾
Create

Projects /  Managed Service Prov... /  WPMSP-1097

**Description**

A deeper analysis on [SATAYO](#) evidences help us to classify the resources exposed on the bot related to [we-online\[.\]com](#). Some of the findings are to be considered **CRITICAL** for the infrastructure security.

**GENESIS**

Using [SATAYO](#) we detected the present of the log 7B034E8C77F92627192802CCCE2AB3DD on Genesis Market, posted on 11th October 2020.

**TECHNICAL ANALYSIS**

This log contains several credentials and cookies related to we-online[.]com resources, even if the OS of the machine and all the other cookies and credentials suggest it is a personal computer. The number of compromised resources is 113.

The most critical service for which **credentials** were found is <https://venus.we-online.com/>.

```

1 https://venus.we-online.com/
2
3 "Login": sergio.fernandes@we-online.ext
4 "Password":
                
```

We tested this evidence, and **it is still valid**, and **no MFA is implemented** for accessing the service.



Resolved ▾ ✓ Done

**SLAs**

6 Sep 03:11 PM ✗ Time to first response within 16h

**Details**

Assignee	 Simone Cagol <a href="#">Assign to me</a>
Reporter	 Francesco Pavanello
Request Type	 Case Notification SATAYO
Organizations	None
Product Category	SI Satayo
Priority	<span style="color: red;">⬆</span> Highest
Due date	None
Microsoft Teams	<a href="#">Contact Jira admin</a>
Components	<a href="#">SI SATAYO</a>
Request participants	 Corvin Schmid  Tobias Beck  René Sander

MG [Add internal note](#) / [Reply to customer](#) / [Inform stakeholders](#)

Pro tip: press **M** to comment

**Managed Service Prov...**  
Service project

-  Queues
-  Service requests
-  Incidents
-  Problems
-  Changes

**OPERATIONS**

-  Change calendar
-  Alerts
-  On-call

**KNOWLEDGE**

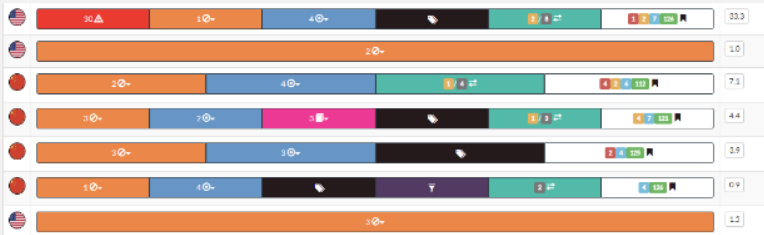
-  Reports

**CHANNELS & PEOPLE**

-  Channels
-  Customers
-  Clockwork Free
-  Checklist

## Hostname

Hostnames are one of the starting points for SATAYO's exposure assessment analysis. This page shows the hostnames found for the selected domain. Each hostname is resolved and its IP is also displayed, along with the country of origin. If a suitcase emoji appears next to an IP address, it means that it is part of a subnet block managed directly by your organization. More on this can be found in the section [Registry](#). If interesting items were found within the hostname, they are shown in the table to the right. Each row also has a score value, and more information about the scoring can be found in the section [Global Report](#).



You can click on each result to explore the item further. A brief description of these subsections is provided below.

## Vulnerability

This page shows the existence of vulnerabilities, identified by a [CVE](#) number and a [CVSS](#) score, on exposed and domain-related resources. For the various CVEs, the link to the U.S. National Vulnerability Database, maintained by the [NIST](#), and an indication of the type of vulnerability listed within [CWE](#), a system of categories used for software weaknesses and vulnerabilities, is given. Links to existing exploits or [PoC](#) are also available.

When you access this page from the [Hostname](#) section, you will only see vulnerabilities related to the IP address you clicked on. Otherwise, you can access this section directly from the menu, where you will see the data for every IP address within the domain. Clicking on one of these IPs will redirect you back to the hostname section, but limited to the selected IP.

## Blacklist host

This page shows the presence of host names within blacklists. This situation can compromise the provision of services and ruin reputations. If browsers or organizations activate controls such as content filtering, the connection to the blacklisted machine may be terminated or refused. Several blacklists allow users to request removal of their resources after a reputation check of the exposed resource.

## SATAYO Items

Hostname

Vulnerability

Blacklist host

Port

Unencrypted protocols

Interesting services

Web server NO SSL ports

Web server ports

Wayback machine

Technologies

robots.txt

HTTP method

SSL/TLS

Registry

Domain related sections

Domain suspicious

Domain correlated

Domain phishing

Domain similar

Domain tld

Potentially confidential data

File

Bucket

GitHub hot data

Mail server

Mobile Apps

Personal information sections

Phone number

General Social

Mail

Breached accounts

# SATAYO guide

- Documentation of all items managed by SATAYO
- Available online, for everyone @ [neteye.guide](#)












```

1 import "vt"
2
3 rule detect_wurth_documents
4 {
5     meta:
6         description = "Detects any documents which contains Wurth information"
7         author = "Giacomo Giallombardo"
8         date = "2022-09-19"
9     strings:
10        $a= /\s(grass\.at|conmetallmeister|arnold-fastening|recanorm|we-online|wuerth-ag|wuerth-industrie|v
11        $b= /\s(wuerthfinance|wurth-international)\s/i
12        $c= /\s(wue?rth)\s/i
13        $d = /\s(confidential)\s|(internal\suse)\s/i
14        $f = /\s(vertraulich)|(für\sden\sinternen\sGebrauch)|(interne\sVerwendung)\s/i
15    condition:
16        ( $a or $c or $b ) and ( $d or $f ) and vt.metadata.new_file
17 }

```

#### LIVEHUNT NOTIFICATIONS

			Edit ▾	Sort by ▾	Filter by ▾
			Detections	Size	First seen
<input type="checkbox"/>	   <span>imdb_tr.csv</span> <span>text</span>	detect_wurth_documents BRANDMONITORING confidential documents	0 / 61	23.28 MB	2022-10-2 20:19:09
<input type="checkbox"/>	   <span>FRFRESH.txt</span> <span>text</span>	brand_protection_artifact_wurth BRANDMONITORING emails	0 / 61	4.20 MB	2022-10-2 08:21:01
<input type="checkbox"/>	   <span>bt_blocklists</span> <span>python</span>	detect_wurth_documents BRANDMONITORING confidential documents	0 / 61	29.71 MB	2022-10-2 07:30:06

# Sandboxes

- Monitoring of what is shared globally
- Brand monitoring
- Study of threats

# Sandboxes





## Sandboxes

Discover the attack surface, keep it monitored, and manage the exposed data over time. React proactively in order to avoid exploits.

(admin)

Rows: 1-25 / 31

Page 1 of 2

Check	Domain	Time	URL	Snippet
	Würth IT wurth.fr	2022-10-21 17:07:24	⚠️ COPY IN ANONYMOUS TAB 66806bb0d2c75d0440dabbd8602c149ae816838da5a45e416d53ad3f88027be6	31 39 36 32 61 73 64 0D 0A 6D 61 72 69 65 2E 65 1962asd.marie.e 62 65 72 *begin_highlight*40 77 75 72 74 68 2E 66 72 *end_highlight*3A 62 63 65 ber*begin_highlight*@wurth.fr*end_highlight*:bce 6C 76 49 5A 38 0D 0A 6D 61 72 6B 65 74 6D 61 6D IVI28.marketmam
	Würth IT we-online.com	2022-10-21 17:07:24	⚠️ COPY IN ANONYMOUS TAB 783ff5bee89f898bf871935c58e7688a1ad444f6613529c487fd87483601bd62	61 6E 75 66 61 63 74 75 72 65 72 3A 20 20 20 20 anufacturer: 20 20 20 20 20 *begin_highlight*20 57 75 72 74 68 20 *end_highlight*45 6C 65 *begin_highlight* Würth *end_highlight* Ele 6B 74 72 6F 6E 69 6B 20 0D 0A 43 6F 6E 74 61 63 ktronik...Contac 64 65 72 73 74 61 6E 64 20 69 73 20 6F 66 20 61 derstand is of a *begin_highlight*20 63 6F 6E 66 69 64 65 6E 74 69 61 6C 20 *end_highlight* 6F 72 *begin_highlight* confidential *end_highlight* or 20 70 72 6F 70 72 69 65 74 61 72 79 20 6E 61 74 proprietary nat 69 63 65 20 73 68 61 6C 6C 20 61 6C 73 6F 20 62 ice shall also b 65 20 74 72 65 61 74 65 64 20 61 73 *begin_highlight*20 43 6F 6E *end_highlight* e treated as *begin_highlight* Con *end_highlight* *begin_highlight*66 69 64 65 6E 74 69 61 6C 20 *end_highlight*49 6E 66 6F 72 6D *begin_highlight*fidential *end_highlight* Inform 69 73 20 41 67 72 65 65 6D 65 6E 74 2E 20 41 is Agreement. A 6E 61 6C 6F 67 20 44 65 76 69 63 65 73 *begin_highlight*20 43 6F *end_highlight* nalog Devices *begin_highlight* Co *end_highlight* *begin_highlight*6E 66 69 64 65 6E 74 69 61 6C 20 *end_highlight*49 6E 66 6F 72 *begin_highlight*fidential *end_highlight* Infor 66 69 64 65 6E 74 69 61 6C 69 74 79 20 6F 66 20 6D 6D 6E 66 69 64 65 6E 74 69 61 6C 20 *end_highlight*49 6E 66 6F 72 6D 61 74 *begin_highlight*dential *end_highlight* Informa 6E 73 65 65 20 28 78 29 20 72 65 71 75 69 72 69 nsee (x) requiri 6E 67 20 61 63 63 65 73 73 20 74 6F *begin_highlight*20 43 6F 6E *end_highlight* ng access to *begin_highlight* Con *end_highlight* *begin_highlight*66 69 64 65 6E 74 69 61 6C 20 *end_highlight*49 6E 66 6F 72 6D *begin_highlight*ential *end_highlight* Informa 20 77 69 74 68 20 72 65 73 70 65 63 74 20 74 6F with respect to *begin_highlight*20 43 6F 6E 66 69 64 65 6E 74 69 61 6C 20 *end_highlight*49 6E *begin_highlight* Confidential *end_highlight* In 66 6F 72 6D 61 74 69 6F 6E 20 61 73 20 74 68 65 formation as the 73 69 6F 6E 2C 20 75 73 65 20 6F 72 20 6B 6E 6F sion, use or kno 77 6C 65 64 67 65 20 6F 66 *begin_highlight*20 43 6F 6E 66 69 64 *end_highlight* wledge of *begin_highlight* Confid *end_highlight* *begin_highlight*65 6E 74 69 61 6C 20 *end_highlight*49 6E 66 6F 72 6D 61 74 69 *begin_highlight*ential *end_highlight* Informati 3B 20 61 6E 64 20 28 69 69 69 29 20 6E 6F 74 20 : and (iii) not 74 6F 20 75 73 65 *begin_highlight*20 43 6F 6E 66 69 64 65 6E 74 *end_highlight* to use *begin_highlight* Confident *end_highlight* *begin_highlight*69 61 6C 20 *end_highlight*49 6E 66 6F 72 6D 61 74 69 6F 6E 20 *begin_highlight*ial *end_highlight* Information
	Würth IT we-online.com	2022-10-21 17:07:24	⚠️ COPY IN ANONYMOUS TAB dfe8273667e0f68d88a67d4d3db41e80ec84b2e9d50fcc427de61eb7ca8b2cb63	30 2C 30 31 36 31 38 37 32 30 34 37 31 2C 2C 2C 0,01618720471,.. 73 61 6C 65 73 2D 75 6B *begin_highlight*40 77 65 2D 6F 6E 6C 69 *end_highlight* sales-uk *begin_highlight*@we-onli *end_highlight* *begin_highlight*6E 65 2E 63 6F 6D *end_highlight*2C 6F 6B 2C 6E 6F 2C 79 65 73 *begin_highlight*ne.com *end_highlight*,ok,no,yes
	Würth IT we-online.com	2022-10-21 17:07:24	⚠️ COPY IN ANONYMOUS TAB 9d96d0ea93e2da8b3bbd38c0a3bbaa2fac80d38b99d0e3fd23593e0d8323b437	66 6F 63 75 73 22 20 76 61 6C 75 65 3D 22 77 69 focus value="wi 72 65 6C 65 73 73 2D 73 61 6C 65 73 *begin_highlight*40 77 65 2D *end_highlight* reless-sales *begin_highlight*@we *end_highlight* *begin_highlight*45 65 6C 68 65 65 6E 6D *end_highlight*22 20 70 6C 61 62 *begin_highlight*online.com *end_highlight* *begin_highlight* *begin_highlight*

# Log Stealer Market Place monitoring

- The number 1 threat at the moment
- Initial Access tactic coverage
- Continuous scraping of the major market places
- We have already avoided potentially devastating data breaches for our customers



 fastfire  
 User

 News  
 CVV  
 Dumps  
 RDP

 LOGS pre-order

Stealer:  System:  Country:  Links:  [Upgraded] -->  ONLY WITH COOKIES:

State:  City:  Zip:

ISP:  Outlook:  Per page:  Vendor:  Price:

Newest  Older...

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Racoon	Sicily ISP: Fastweb SpA	esseshop.it   login.aliexpress.com   it.openprof.com   starsystemsrl.it   upgradeshop.it   certifico.com   starsystemsicilia.com   accounts.google.com   accounts.google.com   decathlon.it   Show more...	-	-	archive.zip	2022.10.20	0.26Mb	de####nt [Diamond]	\$ 10.00	Buy
Vidar	Sicily ISP: INTERBUSINESS	idmsa.apple.com   facebook.com   users.wix.com   portaleargo.it   lefrece.it   coinmarketcap.com   accounts.google.com   192.168.1.1   amazon.com   login.libero.it   Show more...	-	-	archive.zip	2022.10.19	4.80Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Racoon	Lazio ISP: Fastweb SpA	accounts.google.com   registro.iismarconi.net   re15.axioscloud.it   family.axioscloud.it   mediasetplay.mediaset.it   wifi-cont3.uniroma1.it   accounts.google.com   decathlon.it   amazon.it   accounts.autodesk.com   Show more...	-	-	archive.zip	2022.10.04	0.92Mb	Monsterlog [platinum]	\$ 10.00	Buy
Vidar	Piedmont ISP: Mico s.r.l.	accounts.google.com   remotedesktop.google.com   my.speedify.com   remotedesktop.google.com   sso.damanhur.online   accounts.google.com   amazon.com   webmail.aruba.it   topsolid.it   accounts.rhino3d.com   Show more...	-	-	archive.zip	2022.10.16	1.91Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Vidar	Rheinland-Pfalz ISP: Technische Universität Kaiserslautern	auth.opera.com   auth.opera.com   chemie.uni-kl.de   wss.hochschulsport.uni-kl.de   netflix.com   tumblr.com   auth.opera.com   fddb.info   netflix.com   tumblr.com   Show more...	-	-	archive.zip	2022.10.16	0.20Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Vidar	Umbria ISP: Fastweb SpA	accounts.autodesk.com   accounts.autodesk.com   portaleargo.it   hoepliditore.it   webmailmiur.pelconsip.aruba.it   portaleargo.it   hoepliditore.it   accounts.autodesk.com   webassessor.com   my.valoresalute.it   Show more...	-	-	archive.zip	2022.10.15	0.20Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Vidar	The Marches ISP: Netoiip.com srl	eshop.wuerth.it   zoom.us   accounts.google.com	-	-	archive.zip	2022.10.13	0.03Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Redline	Apulia ISP: VODAFONE	amazon.co.uk   192.168.1.3   itch.io   192.168.0.1   areariservata.subito.it   epicgames.com   login.ncsoft.com   lteality.it   bellomokart.com   sso.garmin.com   Show more...	-	-	archive.zip	2022.10.08	0.69Mb	de####nt [Diamond]	\$ 10.00	Buy
Vidar	Lombardy ISP: Telecom Italia S.p.A.	it.nrtk.eu   qwebunsic.zucchetti.com   securelogin.poste.it   gambacicli.com   servizi.calabriasue.it   api.tim.it   prenotaonline.esteri.it   amazon.it   corsigeometri.it   login.libero.it   Show more...	-	-	archive.zip	2022.10.10	0.29Mb	Mo####yf [Diamond]	\$ 10.00	Buy
Racoon	Campania ISP: INTERBUSINESS	mapei.com   centauria.it   secure.vistaprint.it   portal.office.com   itstechnomusic.com   fattureincloud.it   whooming.com   sso.prjteam.com   accounts.google.com   cart.tinydeal.com   Show more...	-	-	archive.zip	2022.10.08	0.24Mb	de####nt [Diamond]	\$ 10.00	Buy

# 3 major Market Place

- Russian Market (2 millions record)
- Genesis Market (450000 record)
- 2Easy Market (600000 record)



# 3 major Market Place

Genesis Market (450000 record)

genesis 89.28 fastfire

Dashboard new Home / Bots

Genesis Wiki

News 21 Bots

Bots 450k+ Extended Search

Generate FP

Orders

Purchases 4

Payments 3

Tickets

Software 7.2|22.2

Profile

Invites 1

Logout

BOT NAME	RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE
8A229B8C8AC0D1F14FB3F23D1D3294B8	<ul style="list-style-type: none"> <li>Adobe</li> <li>Google</li> <li>BancoPostaPrivata</li> <li>Nexi</li> <li>Vodafone</li> </ul>	<ul style="list-style-type: none"> <li>RalphlaurenStore</li> <li>Office365</li> <li>LinkedIn</li> <li>Netflix</li> <li>UPS</li> </ul>	<ul style="list-style-type: none"> <li>timitMail</li> <li>Instagram</li> <li>Ebay</li> <li>Live</li> <li>IBLBanca</li> </ul>
4838F9C4BD4651134D3B5F9E10F63C58	<ul style="list-style-type: none"> <li>N26</li> <li>Live</li> <li>timitMail</li> <li>Vodafone</li> <li>Pinterest</li> </ul>	<ul style="list-style-type: none"> <li>LinkedIn</li> <li>Netflix</li> <li>LidlStore</li> <li>WishStore</li> <li>Twitter</li> </ul>	<ul style="list-style-type: none"> <li>TIMBusiness</li> <li>Google</li> <li>Dropbox</li> <li>Asus</li> <li>Amazon</li> </ul>
0104F2DD9E66E1CF671BE0155D236B7E	<ul style="list-style-type: none"> <li>Yahoo</li> <li>Twitter</li> <li>Kickstarter</li> <li>MEGARIZ</li> <li>Instagram</li> </ul>	<ul style="list-style-type: none"> <li>Amazon</li> <li>AppleStore</li> <li>Liberio</li> <li>ManomanoStore</li> <li>Alibaba</li> </ul>	<ul style="list-style-type: none"> <li>TripAdvisor</li> <li>Findomestic</li> <li>Pornhub</li> <li>SonyEntertainm...</li> <li>Vista...</li> </ul>
6B7EC8902F58B8F87645C4809B8D7AA20	<ul style="list-style-type: none"> <li>Google</li> <li>LinkedIn</li> <li>BancoPostaPrivata</li> <li>Live</li> </ul>	<ul style="list-style-type: none"> <li>Facebook</li> <li>Office365</li> <li>ZalandoStore</li> <li>Findomestic</li> </ul>	<ul style="list-style-type: none"> <li>Zoom</li> <li>Attlassian</li> <li>Amazon</li> </ul>
FB86500D08F0B954AD13246E604F38E	<ul style="list-style-type: none"> <li>PayPal</li> <li>Netflix</li> <li>Groupon</li> <li>HPConnect</li> <li>Ebay</li> </ul>	<ul style="list-style-type: none"> <li>Spotify</li> <li>Instagram</li> <li>SumUp</li> <li>ManomanoStore</li> <li>Live</li> </ul>	<ul style="list-style-type: none"> <li>FattureinCloud</li> <li>Liberio</li> <li>Facebook</li> <li>Vistaprint</li> <li>Zoom</li> </ul>
00DC17105CA00F66466A581C0ED0C58D	<ul style="list-style-type: none"> <li>AppleStore</li> <li>Google</li> </ul>	<ul style="list-style-type: none"> <li>Facebook</li> <li>LinkedIn</li> </ul>	<ul style="list-style-type: none"> <li>Office365</li> <li>timitMail</li> </ul>





# 2023 DEVELOPMENT ROADMAP

**satay**

# Credit card Market Place monitoring

Biden Market (2 millions record)

- News
- Cards
- HOT Cards
- Base Auction
- Rules
- FAQ
- Tickets
- Purchases
- Balance history
- Settings

Link monitor TOR

fastfire | Classic | Balance: 90 | (0 0) +

Base: [Select filter]

CVR range: 0% - 100%

Phone: [Select filter]

City: [Select filter]

Card Type: [Select filter]

Country: [Select filter]

Have address: [Select filter]

Refundable: [Select filter]

Card Level: [Select filter]

Card Holders Name: [Select filter]

Bank: [Select filter]

State: [Select filter]

Email: [Select filter]

DOB: [Select filter]

ZIP codes (line by line): Enter ZIP codes line by line

BIN Price range: \$0 - \$100

Card Brand: [Select filter]

cvv: [Select filter]

SSN: [Select filter]

BINs (line by line): Enter BIN codes line by line

[Apply filter](#)

Select all DeSelect all Buy all [\$0.00]

Seller	Base	CVR	BIN	EXP	Info	zip	State	City	Country	Price
seller15017	[02.11.2022] MIX MQ	45%	458052	05/2027		2623435	HA	N/A	Israel	8.90 \$
seller15017	[02.11.2022] MIX MQ	45%	540659	04/2023		3075	RÜ	Bern	Switzerland	14.24 \$
seller15017	[02.11.2022] MIX MQ	45%	5181162	09/2023		T3G2S1	AB	Calgary	Canada	35.60 \$
seller15017	[02.11.2022] MIX MQ	45%	533317	11/2026		10154	TO	N/A	Italy	21.49 \$
seller15017	[02.11.2022] MIX MQ	45%	552489	08/2023		T3K6L3	AB	Calgary	Canada	35.60 \$
seller15017	[02.11.2022] MIX MQ	45%	497203	09/2023		42500	LE	N/A	France	16.38 \$
seller15017	[02.11.2022] MIX MQ	45%	497874	06/2023		97438	ST	N/A	France	20.47 \$
seller15017	[02.11.2022] MIX MQ	45%	533621	02/2023		T2H1B5	AB	Calgary	Canada	15.35 \$
seller15017	[02.11.2022] MIX MQ	45%	480213	08/2023		42420	KY	Henderson	United States	13.35 \$
seller15017	[02.11.2022] MIX MQ	45%	516815	06/2024		260 51	EK	Skåne Län	Sweden	20.47 \$
seller15017	[02.11.2022] MIX MQ	45%	552490	09/2023		T3E3Z3	AB	Calgary	Canada	35.60 \$
seller15017	[02.11.2022] MIX MQ	45%	499001	09/2023		75014	PA	Paris	France	20.47 \$
seller15017	[02.11.2022] MIX MQ	45%	490836	04/2023		6723	SZ	N/A	Hungary	8.90 \$
seller15017	[02.11.2022] MIX MQ	45%	497378	12/2023		93400	GA	Ile De France	France	14.24 \$
seller15017	[02.11.2022] MIX MQ	45%	492557	12/2023		1400	SK	N/A	Norway	14.24 \$
seller15017	[02.11.2022] MIX MQ	45%	532180	01/2023		2510	DO	Komárom-Esztergom	Hungary	14.24 \$
seller15017	[02.11.2022] MIX MQ	45%	542436	07/2023		1172	BU	N/A	Hungary	35.60 \$
seller15017	[02.11.2022] MIX MQ	45%	532180	06/2024		4130	DE	Hajdú Bihar	Hungary	14.24 \$
seller15017	[02.11.2022] MIX MQ	45%	428312	11/2023		7700	MO	N/A	Hungary	8.90 \$
seller15017	[02.11.2022] MIX MQ	45%	434960	06/2023		1222	VE	Genf	Switzerland	8.90 \$
seller15017	[02.11.2022] MIX MQ	45%	429941	11/2023		4355	KV	Rogaland	Norway	16.38 \$



Messages 30  
Reaction score 4  
Points 8

[Report](#)[Like](#) [Reply](#)

Pirat-Networks

Member

Mar 1, 2022

Messages 30  
Reaction score 4  
Points 8

Apr 6, 2022

🔗 📄 #5

AU \$78 User Million sales company and partner to the sports and live entertainment industry  
IN \$734 Million User a global engineering company providing engineering products to customers in more than 87 countries across various sectors  
US \$699 Million User global provider of technology-enabled business process outsourcing solutions. The company provides omni-channel customer experience management

CA \$1 Billion User School Board is a school district that serves kindergarten to grade 12 students at more than 257 schools in the Region

UK \$816 Million User provides public bus transport services throughout

IN \$321 Million User Alliance Insurance Company Limited), a subsidiary of Finance

IN \$150 Million User PC It provide end-to-end IT services and solutions in India

MX \$8 Million User Group is an international industrial development firm with more than 30 years of experience developing Industrial Parks and Industrial Buildings in Mexica

BR \$100 Million User provides Hosting and Cloud Computing with quality, efficiency and above all safety for the business of its customers who are 24 hours online.

IT \$13 Billion User manufactures underground and submarine cables and systems for power transmission and distribution, as well as medium and low voltage cables

[idk](#)

[Report](#)[Like](#) [Reply](#)

Pirat-Networks

Member

Mar 1, 2022

Messages 30  
Reaction score 4  
Points 8

Apr 9, 2022

🔗 📄 #6

US Corp was founded in 1996. This company provides custom IT services and products. Their headquarters are located in Milpitas, California.

Revenue:

\$1 Billion

IT the transport sector first and then in logistics

Revenue:

\$29 Million

[idk](#)

[Report](#)[Like](#) [Reply](#)

Apr 13, 2022

🔗 📄 #7

написал тебе в токс

# Initial Access Brokers monitoring

- forums scraping
- dorks (attackers use Zoominfo)

# Initial Access Brokers monitoring

- forums scraping
- dorks (attackers use Zoominfo)



Romanians  
HDD-drive

Пользователь

Регистрация: 14.06.2022

Сообщения: 47

Реакции: 5

06.10.2022

Fresh update 40 VNC's South Koreaa  
With full Admin rights , and clean  
200\$  
work only with middle man

Жалоба



Romanians  
HDD-drive

Пользователь

Регистрация: 14.06.2022

Сообщения: 47

Реакции: 5

10.10.2022

150 Fresh RDP's Mix Geo  
All Admin Rights  
All Rdp's Clean ( No Encryption ) 70% Asian Parts and rest EU/US  
70%Admin Workgroups  
30% Local Admin  
All Comes From Exploits ) So they are Uniq NO BRUTE FORCE!  
The Rdp's Can pe also used for Sending Emails ( Direct Delivery / LocalHost / ISP . Smtп Provider ) For inbox

Prize 850\$ All 150 Rdp's

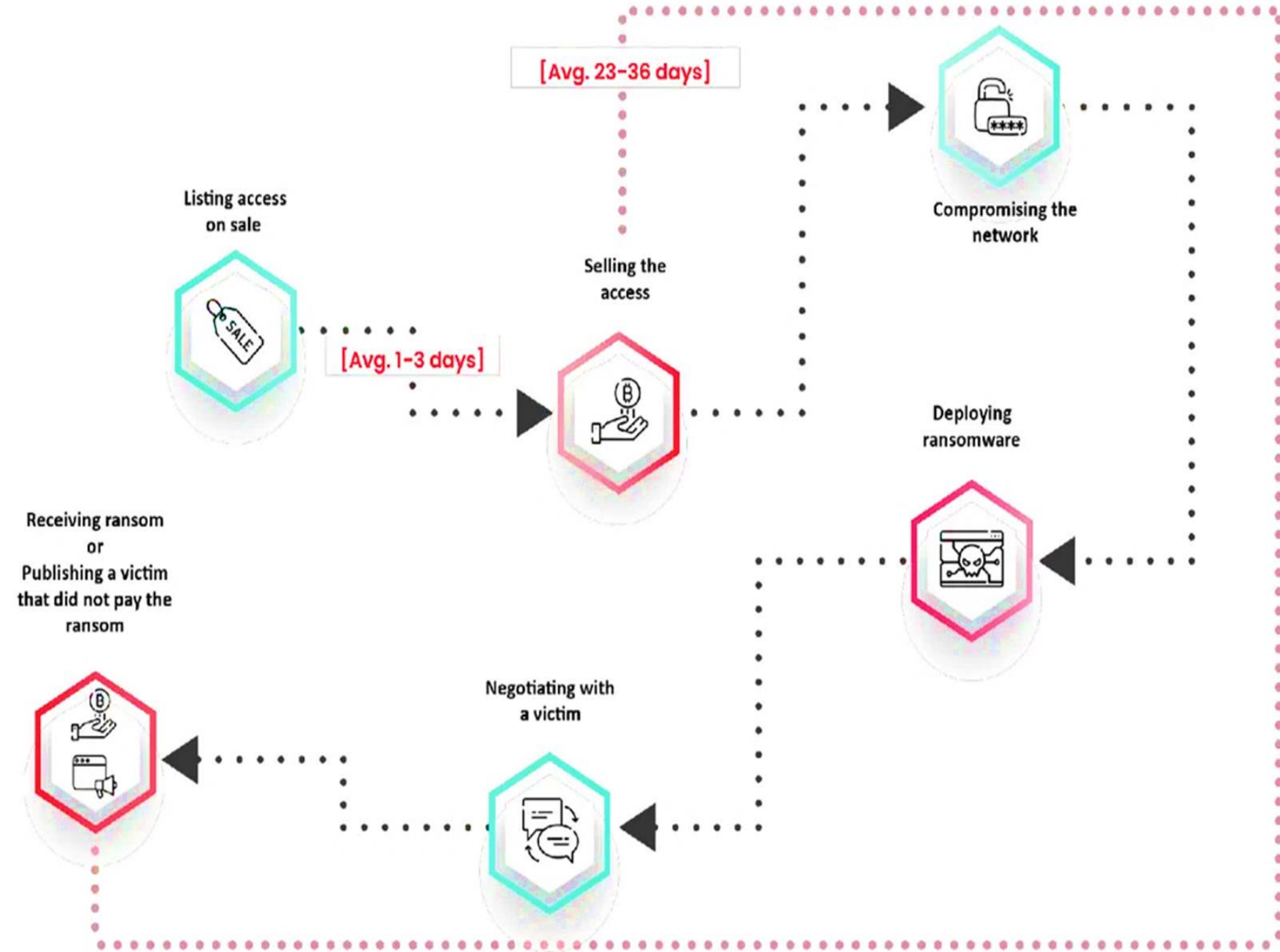
Also i have for Sell South Korea Machines POS terminals ( Maybe Big Corps ) i didn't checked  
\$200 1 Pos Terminal Windows With full Admin Rights  
i Have 50-100 Pc's

Middle Man Accepted Any time

Жалоба

# Initial Access Brokers monitoring

- forums scraping
- dorks (attackers use Zoominfo)



# Mitre Att@ck correlations

match of SATAYO items with Mitre Att@ck Matrix



[MITRE | ATT&CK®](#)
[Matrices](#)
[Tactics ▾](#)
[Techniques ▾](#)
[Data Sources](#)
[Mitigations ▾](#)
[Groups](#)
[Software](#)
[Campaigns](#)
[Resources ▾](#)

[Blog ↗](#)
[Contribute](#)

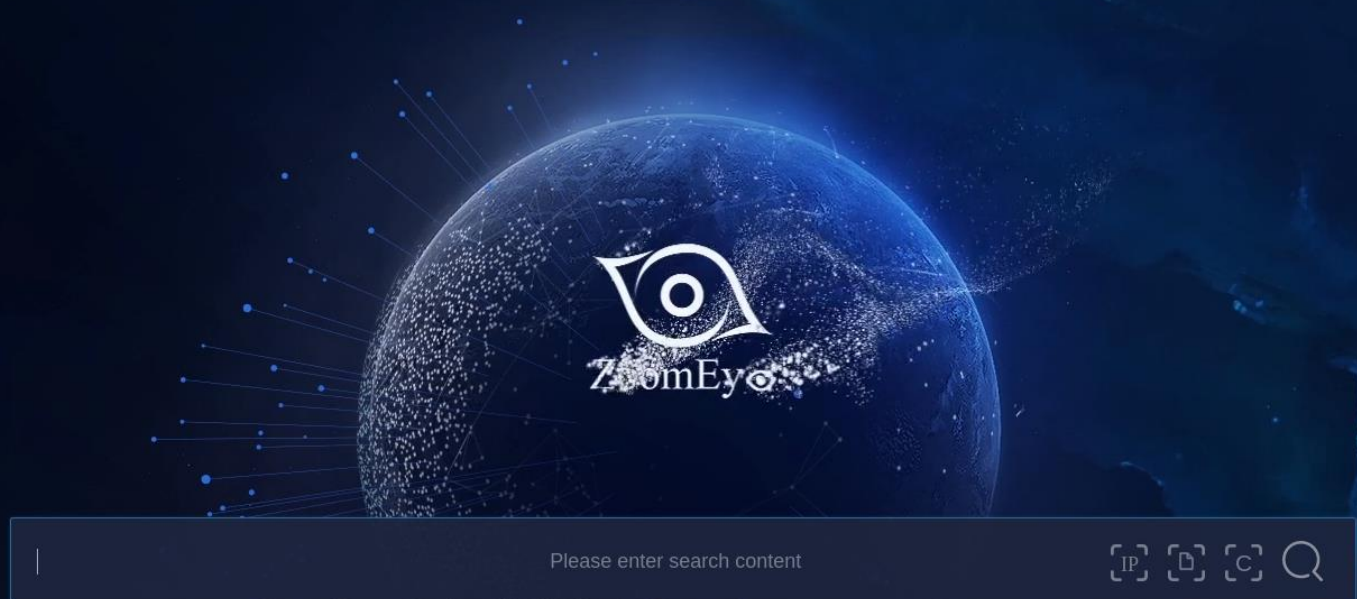
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation Remote Services
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Share Content
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate
Search Victim-Owned Websites			Software Deployment Tools	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)		Domain Trust Discovery	
			System Services (2)	External	Exploitation for Privilege Escalation	Exploitation for Defense Evasion		File and Directory Discovery	
						File and Directory Permissions Modification (2)			



Hosts Search an IP address, name, protocol or field: value

Services: 2.2B IPv4 Hosts: 202.3M IPv6 Hosts: 55.9M Virtual Hosts: 593.1M

ZoomEy [Home](#) [Component](#) [Probe](#) [Discover](#) [Topics](#) [Business](#) [Shared](#) [Manual](#) [Cooperatio](#)



searchTool ▶

[Syntax Description](#) | [Search Config](#)

## Zoomeye / Censys integration

- improve information gathering
- alternative / completion of the visibility provided by Shodan

# Exposure Assessment Index Value

- creation of new metrics
- improvement of existing metrics
- metrics documentation

## ELEMENTS BY MACRO AREAS

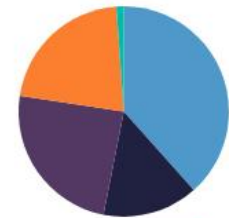
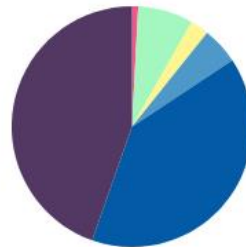
This section summarizes the data, related to the domain, recovered from the various SATAYO research activities. The evidence relates to information gathering activities, active and passive, and is the same that an attacker would carry out in the first phase of the attack. The following evidence therefore allows to simulate the point of view of an attacker, potentially identifying the areas of the organization that already from a surface observation indicate vulnerabilities.

You can print the report (docx format) of the various evidences collected by SATAYO

### INFRASTRUCTURE 42

### DATA, FILES & PEOPLE 20

### DEEP & DARK WEB 41



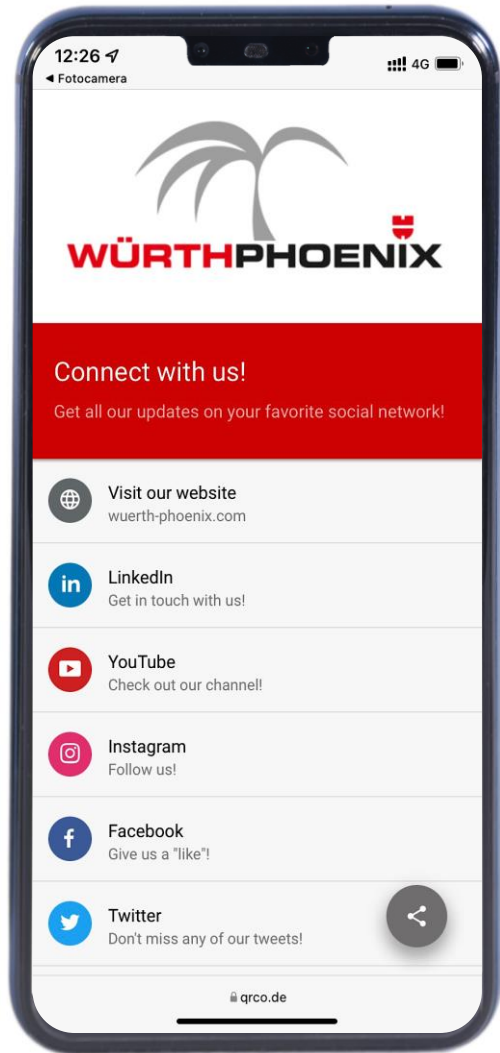


# Our commitment to the community

- owners of deepdarkCTI project  
<https://github.com/fastfire/deepdarkCTI>
- owners of Sigma Rules Crawler project  
<https://github.com/SimoneCagol/sigma-rules-crawler>
- members of Curated Intelligence  
<https://www.curatedintel.org/>
- active contributors to dozens of open source projects  
(dnsrecon, OpenCTI, Holehe, ...)







**CONTACT US**

[www.wuerth-phoenix.com/en/contact-us](http://www.wuerth-phoenix.com/en/contact-us)

[info@wuerth-phoenix.com](mailto:info@wuerth-phoenix.com)

**MORE THAN SOFTWARE**





info@wuerth-phoenix.com  
www.wuerth-phoenix.com



Thank you  
Grazie Danke

#WEINNOVATE