



ZEROFOX®

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

Service To Obtain Legitimate EV Certificates For Threat Actors Advertised

New and untested threat actor “DragonLah” advertised their service to obtain legitimate extended validation (EV) certificates for threat actors on the Russian language Dark Web forum “RAMP”. EV certificates help malicious websites look more trustworthy and pose a risk when leveraged by threat actors. The actor claims that they can obtain the certificates from some of the top Certificate Authorities (CAs), including:

- SSL.com
- Digicert
- GlobalSign
- Certum
- Comodo

The actor further specified that they will deliver the certificates via:

- USB
- RDP
- HSM (including Azure Key Vault and AWS CloudHSM)

Prices for the EV certificates start at \$4,500 USD. The actor also agreed to use an escrow service, indicating a higher likelihood of a successful transaction with buyers.

If this threat proves legitimate, ZeroFox researchers assess that it could pose a major security risk to the public, increasing the chances of successful phishing or malware distribution campaigns.

Original post from threat actor "DragonLah" advertising their service to obtain legitimate EV certificates for threat actors.

Service To Obtain EV Certificates For Threat Actors (Cont.)



DragonLah
May 16, 2022

Messages	2
Reaction score	0
Points	1

Thursday at 7:30 PM

Hello friends,

My team and I have the ability to obtain these certificates because of our understanding of the work of certification centers. I know that there is a high demand for such certificates, and, my friends, I am here to help alleviate some of that demand.

Furthermore, we are ready to offer you (the exploit community) this service.

Services:

EV Cert:

We can create EV code certificates at ANY major certificate authority.

SSL com, Digicert, GlobalSign, Certum, Comodo and any others.

New

<

🔖

#1

New Shop Offers Comprehensive Sets Of PII Related To U.S. Business Owners

ZeroFox researchers recently identified a new English language Deep Web automated marketplace, dubbed “BlackBet”, specializing in the sale of personally identifiable information (PII). Unlike similar shops, this new marketplace offers comprehensive sets of PII related to U.S. business owners. Compromised data includes:

- Owner’s full name
- SSN
- Date of birth
- Articles about the business
- Images of driver’s license
- Background check
- Credit report

The shop has approximately 40 sets of PII related to different business owners available. Prices for these datasets range from \$10 USD to \$20 USD, depending on the information included.

Since the full information of U.S. citizens is highly sought after by threat actors, ZeroFox researchers believe that the emergence of this new marketplace could lead to an increase in identity theft or loan and relief fraud.

A screenshot of the new English language Deep Web automated marketplace, dubbed "BlackBet".

New Shop Offers PII Related To U.S. Business Owners (Cont.)

BlackBet <<

Business_Fulls OWNER_SSN+DOB+articles+DL+BG+CR The market page. Here you can buy different SSNs

GENERAL

News

MARKET

Shops

Banks

Personal Info

- SSN/DOB/DL/CS/BG/CR
- PROs with photo DL
- Business_Fulls
- OWNER_SSN+DOB+articles+DL+BG+CR
- SSN+DOB+DL+B/A R/N + Employment

Lookup Info >

Filters

Add to cart everything from the page SHOW FILTERS

Company Name	State	Form/TYPE	Principal office street address	Articles	DL front	DL BACK	BG	CR	Seller	Price	Actions
CAJ Real Estate, LLC	TX	LLC	408 WEST 17TH STREET, STE. 101, AUSTIN, TX 78701	No	No	No	Yes	No	BIZZ_FULZZ	\$15	
KAS PAINTING LLC	FL	LLC	4276 E 10 CT, HIALEAH, FL 33013	No	No	No	Yes	No	BIZZ_FULZZ	\$15	
KEYS KIRO, LLC	OH	LIMITED LIABILITY COMPANY	115 MILNER RD, GRANVILLE OH 43023	Yes	Yes	Yes	Yes	No	BIZZ_FULZZ	\$40	
Wyoming Royalties, Inc	WY	Profit Corporation	6175 W Incline Rd, Casper, WY 82604	Yes	Yes	Yes	Yes	No	BIZZ_FULZZ	\$40	
HOST SERVICES, INC	MD	Profit Corporation	6905 ROCKLEDGE DRIVE, BETHESDA, MD 20817	Yes	Yes	Yes	Yes	No	BIZZ_FULZZ	\$40	

Malware Loader Runs On Windows Machines

New and positively trending threat actor “lucrostm” advertised their malware loader that runs on Windows machines, on the English language Deep Web forum cryptbb[.]com. The actor claims that the loader exploits local system binaries (LOLBins) to achieve and maintain persistence. According to the actor, the loader allows operators to download and execute additional payloads on compromised machines while evading most antivirus products.

Additional features of this loader include:

- Will not run in a virtual machine (VM) or debugger to avoid analysis and reverse engineering
- Built on serverless architecture, making attribution more difficult

Prices for the loader vary, depending on the length of the license, including:

- \$360 USD for lifetime
- \$30 USD for one-month

The actor also said they were willing to negotiate a price for the source code, with offers starting at \$880 USD.

Original post from threat actor "lucrostm" advertising their malware loader that runs on Windows machines.

Malware Loader Runs On Windows Machines (Cont.)

[\[SOURCE/BUILD\]](#) [\[Go\]](#) **Super Stealthy Remote Access Tool (Windows)**



lucrostm •
Junior
Member

Posts: 5
Joined: Mar 2022
Reputation: 3

#1

06-10-2022, 03:09 PM

What is it and what's its purpose?
This malware grants the attacker a persistent entry point to introduce other malware and tools. Why? Let's say you get to your target directly with a RAT but it gets detected, now you have to start again with probably even a lesser chance of having success. With this tool instead you have no chance of being detected and you can do/download everything you want on your target. It is scalable and can be used in any environment.

How?
Using an innovative persistence technique it hides and bounces, if somehow it gets caught during execution or in the file system, no worries, it will be ready again at the next start-up.
The malware dissociates from any action it takes by carefully utilizing LOLBINS, such that it will not be held accountable for installing other malware by anti-malware solutions. So you can fuck around and not find out 😊

Actor Claims Access To Two Different Critical Infrastructure Systems In Europe

New and untested threat actor “CycloneOrg” advertised access to the internal networks of two different critical infrastructure systems in Europe, on the English language Deep Web forum cryptbb[.]com. The actor claims to have access to administrator panels for both a dam in Italy and an aqueduct in Sweden.

The actor claimed that individuals with access to the dam would be able to operate industrial control systems, including the ability to open floodgates.

The actor further claimed that individuals with access to the aqueduct would have capabilities to control the water temperature, manipulate chemical compounds in the water, and tamper with alarms.

ZeroFox cannot rule out the possibility that this is a scam due to the actor’s lack of credibility on the forum. Our researchers note that SCADA systems were often targeted by ransomware gangs in 2021, but most of these were located in the U.S.

Original post from
threat actor
"CycloneOrg"
advertising access to
the internal networks
of two different critical
infrastructure systems
in Europe.

Actor Claims Access To Critical Infrastructure Systems (Cont.)

