



| Flash |

New Extended Validation Code Signing Service Advertised

F-2024-07-03a

Classification: TLP:CLEAR

Criticality: Low

**Intelligence Requirements: Deep and Dark Web, Threat Actor, Malware,
Phishing**

July 3, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on July 3, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | New Extended Validation Code Signing Service Advertised

➤ Key Findings

- On June 30, 2024, untested actor “enryu” advertised a new extended validation (EV) code signing service on the primarily Russian-speaking dark web forum exploit.
- According to the advertisement, illicit validation certificates can be purchased, which allow malicious webpages to bypass security protocols such as SmartScreen, Windows User Account Control, and Windows Defender, as well as some antivirus (AV) software provided by third parties such as Kaspersky, Avast, and Malwarebytes.
- Illicit validation certificates offer cyber threat actors the ability to augment a wide array of malicious activities, such as the deploying of disruptive malware to target networks, enhanced social engineering attacks, or data theft resulting in operational disruption, extortion or fraud.
- Given the versatility offered by initial network access, services such as these are very likely to appeal to a wide range of threat actors with varying intents and motivations, leading to their continued development, competitiveness, and innovation.

Details

On June 30, 2024, untested actor enryu advertised a new EV code signing service on the primarily Russian-speaking dark web forum exploit. According to the advertisement, illicit validation certificates can be purchased, which allow malicious webpages to bypass security protocols such as SmartScreen, Windows User Account Control, and Windows Defender, as well as some AV software provided by third parties such as Kaspersky, Avast, and Malwarebytes.

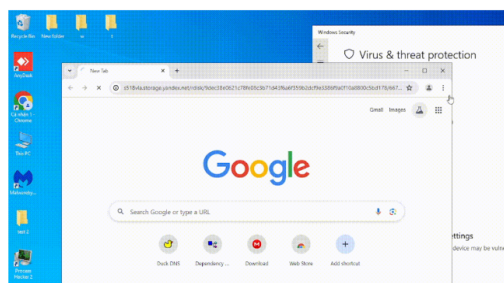
- Compared to SSL/TLS encrypted web pages certified with domain validation (DV) or organization (OV) certificates, those with extended validation (EV) provide a higher level of verification security assurance.
- EV certified web pages often offer the interacting end user visual reassurance, such as the requested URL being preceded by a green padlock and the organization's name. They are also much less likely to trigger alerts from the operating system or third party security software programmes. Both of these translate to higher levels of endorsement and subsequent end user trust.
- Enryu's orders are allegedly completed within 24 hours, and available to a single buyer only. This is a faster turnaround than that offered by many competing services, which typically range between two and five days.

EV CODE SIGNING CERTIFICATES VALID

With code signing, users can trust the software they are downloading, and need not worry about downloading malware onto their computer. A code signing certificate issued by a trusted certificate authority.

What is EV Code Signing?

- Instant bypass of SmartScreen filter, no reputation required
- Makes UAC trusted
- Signed software inspires more trust in the user, which significantly increases conversion
- Bypass of some antiviruses based on signature detection



Exploit post advertising new EV code signing service

Source: ZeroFox Intelligence

According to enryu, a single certificate costs USD 500, with other options of “one week” and “one month” advertised for USD 1,500 and USD 2,900, respectively. While it is not specified what these services relate to, is it likely the length of time for which a certificate is valid.

If this is the case, enryu’s service is slightly more expensive than others observed by ZeroFox, which typically charge between USD 1,500 and USD 3,000 for a single certificate valid for one year, depending on the certificate authority. There is a roughly even chance that enryu’s higher price is due to the ability to bypass additional security protocols.

Certificates in stock or on order

- Certificates by pre-order: production time 24h
- Discussion of wholesale orders
- Certificates are sold strictly to one person. Fresh and unused

Bypass ALL AV

 Features

- ♥ Bypass Windows Defender
- ♥ Bypass Kaspersky
- ♥ Bypass MalwareBytes
- ♥ Bypass Avast
- ♥ Bypass 360 Safeguard
- ♥ Bypass Avira
- ♥ Bypass Baidu
- ♥ Bypass AVG
- ★ Memory Injection
- ★ Encryption
- ★ (ETW) Bypass
- ★ (AMSI) Bypass
- ★ Virtual Machine Bypass
- ★ Stable

Contacts

TG Channel: https://t.me/Baphomet_Crypter
Owner: @Baphomet_AV

Exploit post advertising new EV code signing service

Source: ZeroFox Intelligence

Illicit validation certificates offer cyber threat actors the ability to augment a wide array of malicious activities, such as the deploying of disruptive malware to target networks, enhanced social engineering attacks, or data theft resulting in operational disruption, extortion, or fraud. To enable this, they attract victims to malicious web pages by leveraging techniques such as SMS and email phishing, domain spoofing, and if the web

page is able to establish a positive reputation-search engine optimization (SEO) poisoning.

- Threat actors almost certainly seek to leverage illicit validation certificates in as many separate, lucrative attacks as possible, to justify their price tag. However, they are sought after and often revoked by certificate authorities, web browser vendors, and threat researchers.
- EV-certified web pages do not implicitly enable hosted files that are downloaded by the end user to bypass the same security protocols. There is a roughly even chance that downloaded files will be scrutinized by security software regardless of their originating location.

Given the versatility offered by initial network access, services such as these are very likely to appeal to a wide range of threat actors with varying intents and motivations, leading to their continued development, competitiveness, and innovation.

Recommendations

- Organizations should implement training for employees, focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.
- Reduce the impact of phishing attacks by ensuring networks and associated accounts are configured according to the principle of least privilege.
- Scrutinize digital communications, even if appearing to have originated inside the organization. Look for incorrect or unusual grammar, spelling mistakes, mismatched hyperlink URLs, and illegitimate sender addresses.
- Individuals and network endpoints should be granted only the minimum level of access and permissions needed to conduct a specific role.
- Organizations of all sizes and industries should implement a company-wide comprehensive multi-factor authentication (MFA) policy. As the most secure form of MFA, physical authentication devices should be used where possible. Devices such as USB and public key infrastructure (PKI) keys are the least susceptible to interception, tampering, or compromise.
- MFA challenges should be as regular as possible, without causing significant disruption or the frustration likely to lead to misuse.
- Organizations should ensure their web pages and other online content are protected by using secure coding practices and updated security plugins and scrutinized with regular website security audits.
- Organizations should ensure that digital assets that make up technology stacks and attack surfaces are regularly updated as a part of a thorough patch-management process.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%