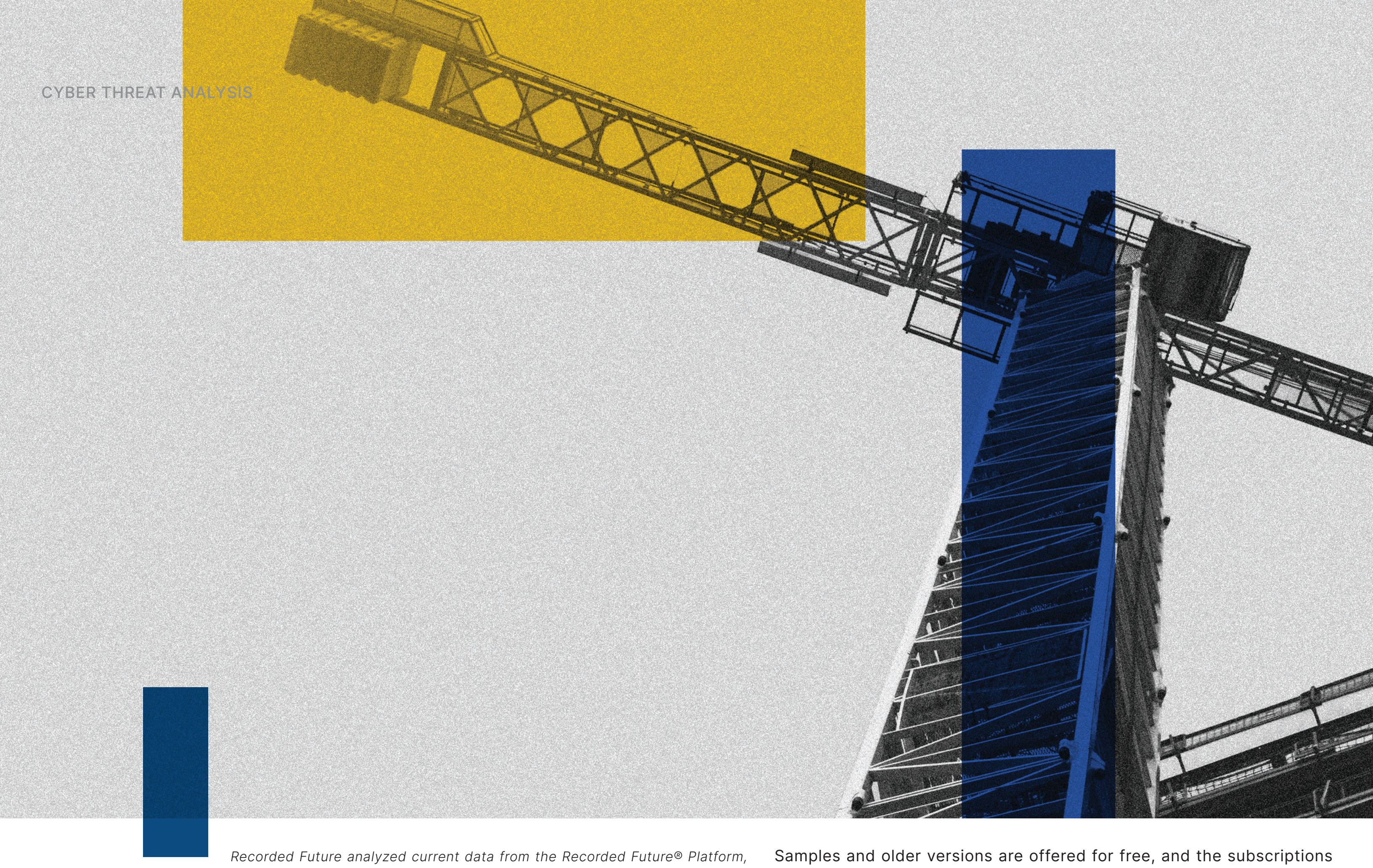
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-0721

USER-FRIENDLY LOADERS AND CRYPTERS SIMPLIFY INTRUSIONS AND MALWARE DELIVERY



Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other open source intelligence (OSINT) sources to identify loaders and crypters that facilitate threat actor campaigns. This report expands upon findings addressed in the report "Automation and Commoditization in the Underground Economy," following reports on database breaches and on checkers and brute forcers. This report will be of most interest to network defenders, security researchers, and executives charged with security risk management and mitigation. Dark web sourcing for this research is available to Recorded Future clients.

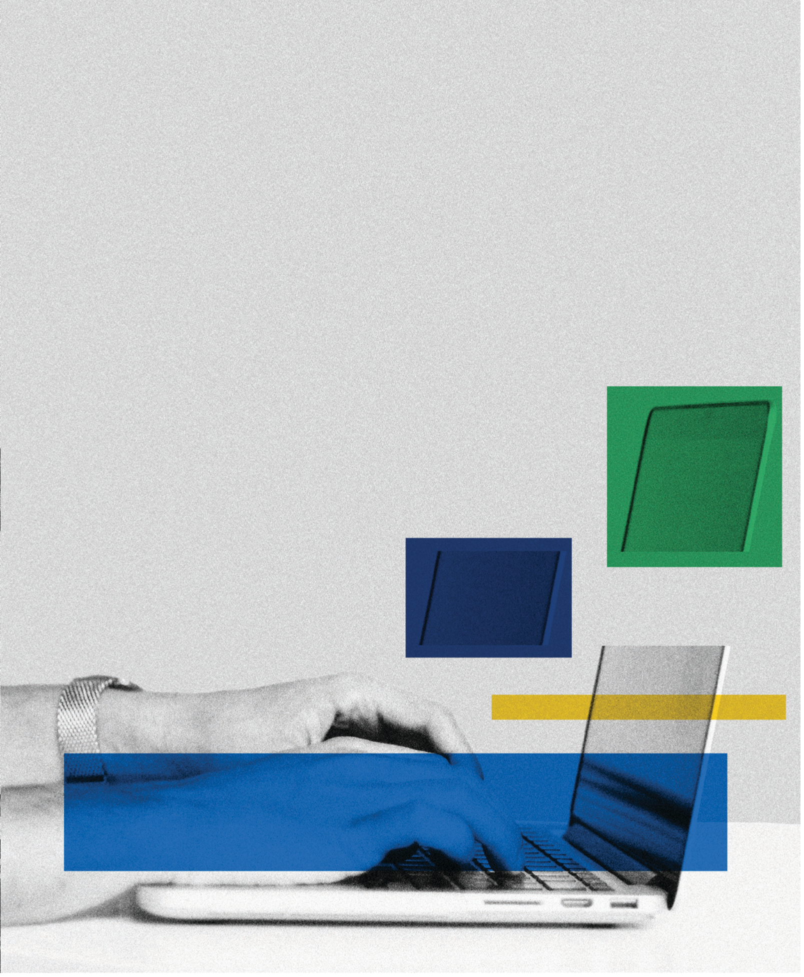
EXECUTIVE SUMMARY

In our February 2020 report "Automation and Customization in the Underground Economy," we identified automated services and products produced by threat actors and developers that facilitate criminal activities. This report dives further into loaders and crypters, identifying popular loader variants within select dark web forums and analyzing widely used crypters via clearnet domains, as well as providing mitigation strategies to identify loaders and crypters attempting to intrude into your network.

Loaders and crypters are an example of products and services that operate in tandem to elude network security settings, maintain presence on impacted machines and networks, and encrypt malicious payloads to masquerade intent. Executing malware on a victim's machine while remaining undetected by antivirus software usually requires some technical skill, but there is a growing trend for these products to be offered as services by developers who provide user support, easy-to-use interfaces, and regular updates in response to new antivirus features in return for subscription fees rather than one-time purchases. Samples and older versions are offered for free, and the subscriptions are increasingly affordable (tens or hundreds of dollars a month rather than thousands), making it easier than ever for threat actors with limited technical knowledge to execute attacks.

KEY JUDGMENTS

- Developers of loaders and crypters are creating products and offering services that are customizable, automated, and designed to be user-friendly to cater to non-technical users.
- Threat actors are using loader and crypter services to elude network security settings and to encrypt and obfuscate payloads that propagate malware.
- Threat actors are discussing specific loader variants on different forums, with SmokeLoader and Amedy Loader being widely advertised and discussed.
- Threat actors are directing forum users to clearnet domains that advertise crypting services, with Moon Crypter and Saddam's Crypter variants identified as containing multiple encrypting capabilities with an easy-to-use interface.



Background

Once threat actors have identified a target, their next step is frequently to deliver the malicious payload to the target system or device. Since many of the targeted systems or devices are protected to some extent by antivirus software, which may recognize, flag, or block the malicious payload, threat actors typically use special tools such as loaders and crypters as part of the initial infection. These tools are designed to elude detection by endpoint security products, and then download and execute one or more malicious payloads.

As the number of attack surfaces (connected devices) has continued to increase, more threat actors are using innovative attack vectors to deploy new variants of malware. Some of these threat actors do not possess technical expertise or are not dedicated to maintaining their own crypter or loader; thus, they turn to more technically savvy threat actors to develop, maintain, and offer these services. Given these needs, developers of loaders and crypters have capitalized on the market demand for these services by providing customized products and "turnkey solutions."

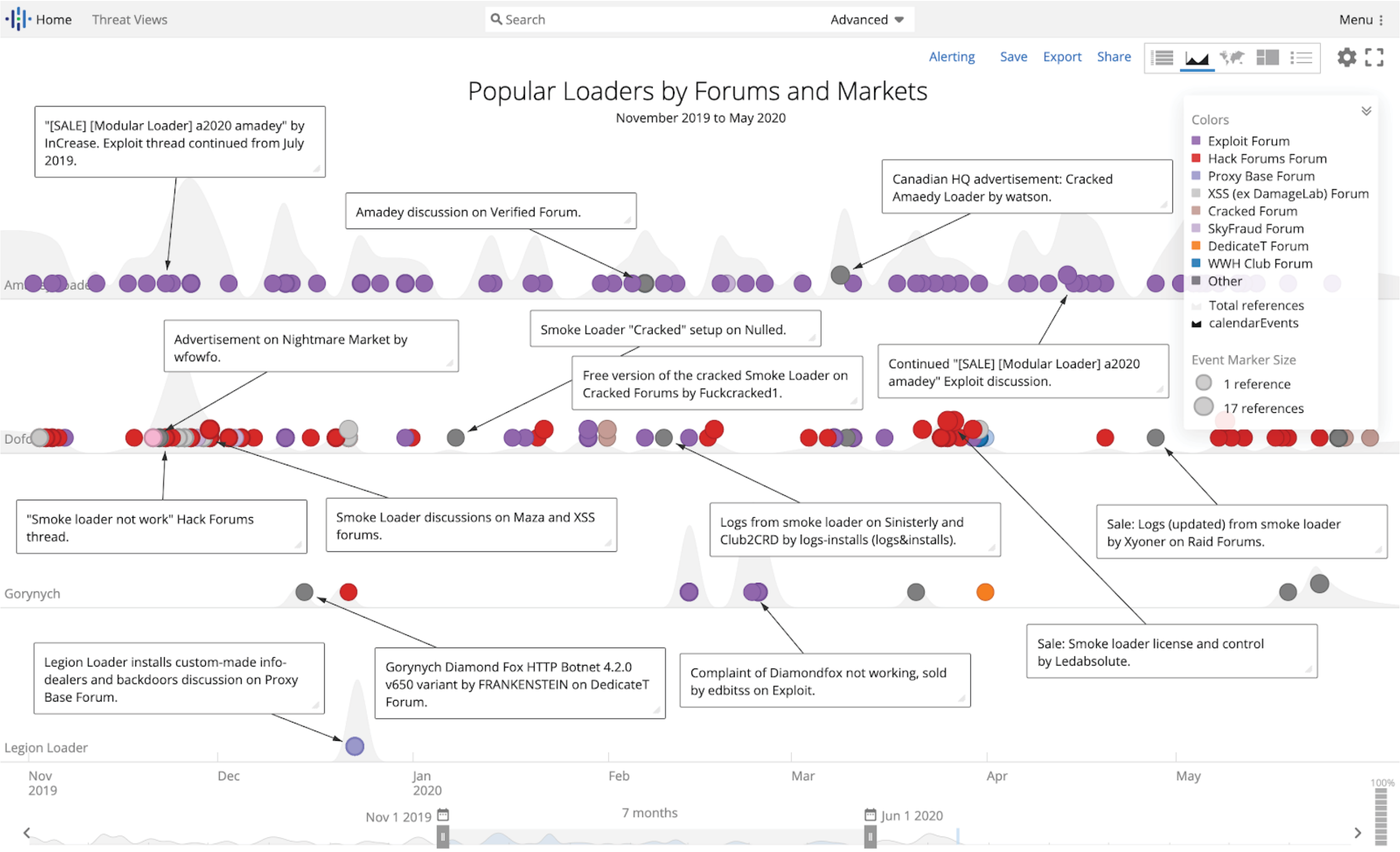
Loaders

Loaders usually contain a limited set of capabilities. They are generally responsible for surveying a victim's computer, checking in with a command and control (C2) server, and then downloading and executing more advanced malware. The exact details of this process vary from loader to loader, but the most basic loaders might save the final payload to the victim's file system and then run it as a new process. The most advanced loaders will keep the downloaded payload entirely in-memory, and execute it using a process injection technique like process hollowing or reflective DLL injection. By keeping the payload in memory, the loader reduces the chances that security products could detect the final payload.

Not all loaders are offered for sale, however. Some of the most effective loaders, such as Pony Loader and Trickbot, are under the control of advanced threat actors, and while we identified threat actors discussing vulnerability exploitation, activities, and capabilities associated with those and other well-known loaders, we did not find threat actors advertising control of or renting these loaders as a service. They are not likely to be openly advertised across dark web forums or markets for the foreseeable future.

In April 2020, an open source reported that Emotet is being offered as a malware-as-a-service option by threat actors, resulting in a 145 percent increase in Emotet-related incidents globally from October to December 2019. While open source reporting indicates that Emotet-as-a-service (EaaS) exists, on dark web forums, we observed threat actors acting cautiously rather than recommending legitimate EaaS services due to scamming activities.

Besides these exceptions mentioned above, threat actors are advertising customizable loaders for purchase and free variants across multiple dark web forums and markets. Among these variants, some are more popular and sought after than others. For example, Exploit Forum participants were found to mostly discuss Amadey Loader, while SmokeLoader was widely advertised and discussed across more than six different forums over a six-month period, including XSS Forum, Exploit Forum, Nulled Forum, and English-language forums that cater to more entry-level hackers such as Hack Forums and Cracked Forum.



"[SALE] [Modular Loader] a2020 amadey" by InCrease. Exploit thread continued from July 2019.

Amadey discussion on Verified Forum.

Canadian HQ advertisement: Cracked Amaedy Loader by watson.

Advertisement on Nightmare Market by wfowfo.

Smoke Loader "Cracked" setup on Nulled.

Free version of the cracked Smoke Loader on Cracked Forums by Fuckcracked1.

Continued "[SALE] [Modular Loader] a2020 amadey" Exploit discussion.

"Smoke loader not work" Hack Forums thread.

Smoke Loader discussions on Maza and XSS forums.

Logs from smoke loader on Sinisterly and Club2CRD by logs-installs (logs&installs).

Sale: Logs (updated) from smoke loader by Xyoner on Raid Forums.

Legion Loader installs custom-made info-dealers and backdoors discussion on Proxy Base Forum.

Gorynych Diamond Fox HTTP Botnet 4.2.0 v650 variant by FRANKENSTEIN on DedicateT Forum.

Complaint of Diamondfox not working, sold by edbitss on Exploit.

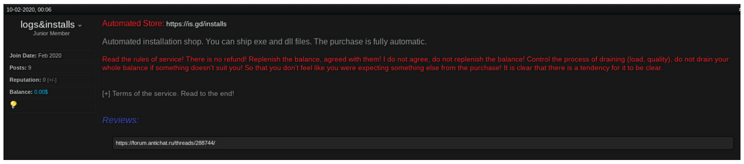
Sale: Smoke loader license and control by Ledabsolute.

Loader variants and forum references from November 2019 to May 2020 (Source: Recorded Future)

Threat Analysis: SmokeLoader

SmokeLoader is a loader family that goes by several names, including Dofoil and Shakif, but most prominently after its namesake proprietor, a threat actor named "SmokeLdr." SmokeLdr has continued to develop the malware, introducing new features to forum members and attempting to stay ahead of security solutions. While SmokeLdr is known to only sell to Russian-speaking individuals in popular forums such as Exploit Forum, there are other sellers. Here are a few examples we've seen:

1. In January 2020, threat actors on Cracked Forum shared a free downloadable SmokeLoader variant that was described as cracked and included a control panel, content screenshots, and built-in anti-VM capabilities.
2. In February 2020, one threat actor advertised their automated shop on Club2CRD Forum, which included access to databases of logs from AZORult, Raccoon Stealer, and SmokeLoader. The threat actor first operated their shop at logs-store[.]com (now defunct) before moving operations to shop1[.]host. We also observed similar advertisements from the same threat actor on Sinisterly Forum and Exploit Forum.
3. In March 2020, another threat actor began posting advertisements for licensing control for their SmokeLoader variant on Hack Forums. The variant is described as "not cracked" and included features like full transfer to a domain of the user's choice, latest version of software, full installation and management, and access to bulletproof domains and VPS. The license was priced at $200 USD.


10-02-2020, 00:06

logs&installs
Junior Member

Join Date: Feb 2020
Posts: 9
Reputation: 0 [+/-]
Balance: 0.00$

Automated Store: https://is.gd/installs

Automated installation shop. You can ship exe and dll files. The purchase is fully automatic.

Read the rules of service! There is no refund! Replenish the balance, agreed with them! I do not agree, do not replenish the balance! Control the process of draining (load, quality), do not drain your whole balance if something doesn't suit you! So that you don't feel like you were expecting something else from the purchase! It is clear that there is a tendency for it to be clear.

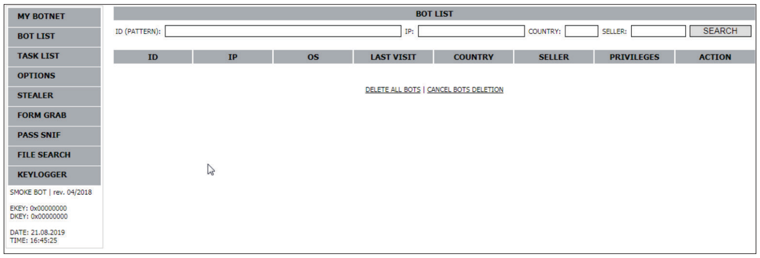
[+] Terms of the service. Read to the end!

Reviews:

https://forum.antichat.ru/threads/288744/

Post by logs&installs for their shop at shop1[.]host (Source: Club2CRD)

SmokeLoader is a very evasive malware, using ever-changing obfuscation and anti-debugging and anti-analysis tactics to frustrate analysts. It can be delivered by a number of means, including exploit kits and email attachments, and is executed using techniques such as process hollowing, embedded shellcode, or PROPagate injection.



SMOKE BOT | rev. 04/2018

EKEY: 0x00000000
DKEY: 0x00000000

DATE: 21.08.2019
TIME: 16:45:25

SmokeLoader panel (2019)

Like many other loaders, the admin interface of SmokeLoader is designed to be relatively simple for buyers to use (shown above). While well obfuscated, the malware is prolific in campaigns, with upwards of 80,000 individual infections occurring in some incidents on March 6, 2018, according to Microsoft. When SmokeLoader is delivered as an executable, it is often packed with multiple layers to obfuscate the code.

Crypters and No-Distribute Scanners

Crypters and no-distribute scanners are two essential services for threat actors involved in propagating malware. Crypting services are used to encrypt and obfuscate malware payloads to avoid detection by antivirus software. Crypters can compress executables to reduce the size of the deliverable, evade sandboxing through virtual machine detection, and masquerade as normal software. No-distribute scanners can then be used to check if the crypted malware is being detected by any antivirus software.

Developers of crypters create products designed to be used by threat actors of varying technical sophistication. These crypters are often user friendly and provide a simple interface that includes a GUI which configures all the options, including encryption methods, keys, and where to inject the payload. Once a threat actor has selected a crypter and uploaded the necessary information, the following generally happens:

- The crypter encrypts the malicious payload into a functioning code.
- The threat actor delivers this program to victims via phishing or spamming.
- The crypter decrypts itself and releases the malicious payload once executed.

We observed threat actors advertising unspecified crypters as part of "package deals" that have been identified including malware variant(s), hacking tools, and other information, and also referring users to crypters or no-distribute scanner services available on Tor and clearnet websites.

Crypters-as-a-Service for Novice Threat Actors

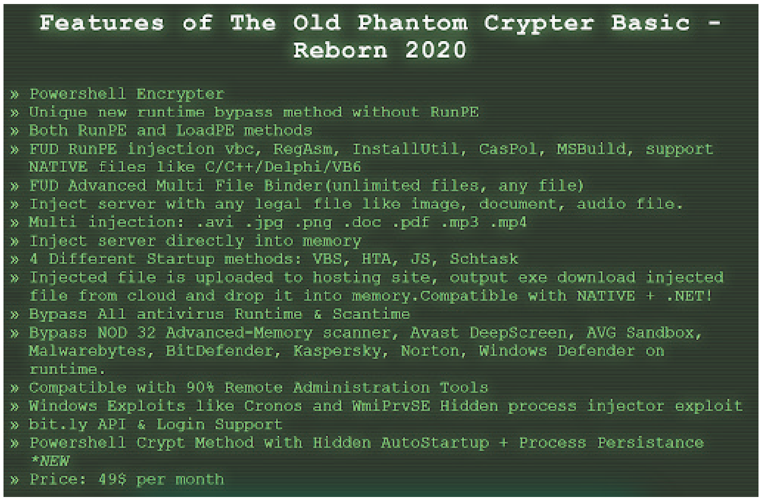
In addition to advertising a product to novice threat actors who lack technical expertise, developers of crypters are capitalizing on the fact that their products require regular updates in response to enhancements in firewall and security network applications. These sorts of quality-of-life updates mean that users of crypter services do not need to devote efforts to defeat security updates when developers of crypters are already providing this service. Although we found some crypters that are available for one-time purchase and do not feature developer support, the most reputable and recommended across dark web sources are the crypters-as-a-service (CaaS) that are predominantly available via clearnet websites.

An entry-level cybercriminal is likely to have no issue in identifying potential samples of freely available crypters on dark web forums that have no barriers to entry. We identified several posts containing bundles of crypters that are freely available for interested parties to download at no additional cost. These bundles often contain no less than ten free samples of different crypters. Though the crypters in these bundles are not as actively supported as other modern crypter services, they are very likely to assist threat actors who are either attempting to learn the fundamentals of reverse engineering or to obfuscate custom malware they either created themselves or purchased elsewhere within threat operations.

Differences Between Products Offered on Open Sources and Dark Web

We saw threat actors advertising crypter services that were often not exclusively available within underground networks or via Tor hidden services (Onion domains) but also on open sources. One sample bundle we saw originated from a crypter service advertised within an English-language underground forum that is accessible via a clearnet website, with no restrictions in place to deter threat actors interested in purchasing access to the service for $49 USD per month. While we did observe exceptions to this rule on multiple high-tier, Russian-language forums where crypter services could range from hundreds to thousands of dollars, the average price of similar services was predominantly under $100 USD per month.

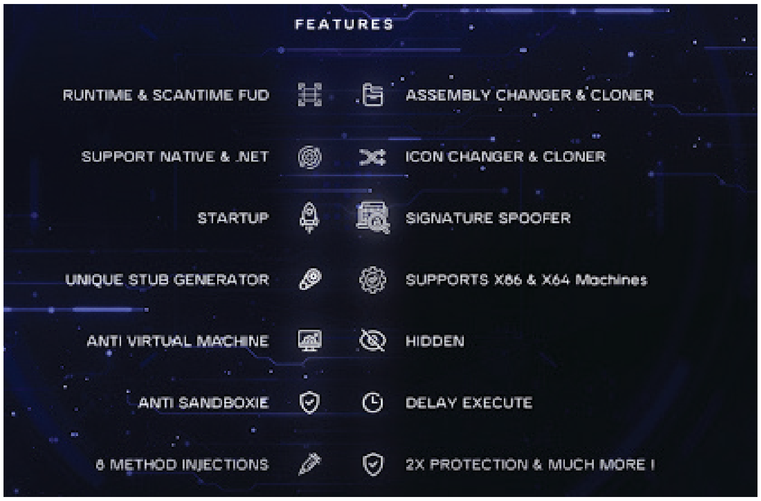
Operators of clearnet crypters do specify that they do not encourage the use of their product or services for malicious purposes, but likely recognize that this does not deter threat actors and overlook this possibility in an attempt to maintain an active, revenue-generating service. On underground forums, it is customarily required for threat actors to engage directly with the vendors to transfer funds and gain access to crypters.



```
Features of The Old Phantom Crypter Basic -
Reborn 2020

» Powershell Encrypter
» Unique new runtime bypass method without RunPE
» Both RunPE and LoadPE methods
» FUD RunPE injection vbc, RegAsm, InstallUtil, CasPol, MSBuild, support
  NATIVE files like C/C++/Delphi/VB6
» FUD Advanced Multi File Binder(unlimited files, any file)
» Inject server with any legal file like image, document, audio file.
» Multi injection: .avi .jpg .png .doc .pdf .mp3 .mp4
» Inject server directly into memory
» 4 Different Startup methods: VBS, HTA, JS, Schtask
» Injected file is uploaded to hosting site, output exe download injected
  file from cloud and drop it into memory.Compatible with NATIVE + .NET!
» Bypass All antivirus Runtime & Scantime
» Bypass NOD 32 Advanced-Memory scanner, Avast DeepScreen, AVG Sandbox,
  Malwarebytes, BitDefender, Kaspersky, Norton, Windows Defender on
  runtime.
» Compatible with 90% Remote Administration Tools
» Windows Exploits like Cronos and WmiPrvSE Hidden process injector exploit
» bit.ly API & Login Support
» Powershell Crypt Method with Hidden AutoStartup + Process Persistance
  *NEW
» Price: 49$ per month
```

Clearnet crypter service bundle ($49 USD per month) (Source: theoldphantom[.]net)



FEATURES

RUNTIME & SCANTIME FUD	ASSEMBLY CHANGER & CLONER
SUPPORT NATIVE & .NET	ICON CHANGER & CLONER
STARTUP	SIGNATURE SPOOFER
UNIQUE STUB GENERATOR	SUPPORTS X86 & X64 Machines
ANTI VIRTUAL MACHINE	HIDDEN
ANTI SANDBOXIE	DELAY EXECUTE
8 METHOD INJECTIONS	2X PROTECTION & MUCH MORE !

Clearnet crypter service bundle ($49 USD per month) (Source: theoldphantom[.]net)

Another modern crypter service that Insikt Group observed being advertised on Hack Forums in December 2019 by member "R A Z" was the eponymous "RAZ crypter" tool, which has continued to generate positive feedback at the time of this writing. Other threat actors on the forum advertising separate commodities such as remote access trojans (RATs) have cross-promoted this particular tool and encouraged buyers interested in their malware to use the service should they need to obfuscate their malware. This spirit of cooperation is not a new phenomenon, with notorious ransomware operators such as the operators of GandCrab ransomware announcing a partnership with NTCrypt, another malware crypter service. NTCrypt achieved the honor by winning an underground "crypt competition."

Written in C#, RAZ crypter was advertised as fully undetectable (FUD) and designed to work with the Remcos, Quasar, and Warzone RATs. Like many other crypters, videos demonstrating bypass of antivirus systems including Kaspersky, ESET, Windows Defender, and Avast were also uploaded to YouTube by the author to demonstrate its effectiveness. The tool is being rented for $25 USD for one month or $40 USD for three months, accepting Perfect Money and Bitcoin payments.

The features shown below in connection to the RAZ crypter incorporate many of the baseline requirements that many crypter services need to offer in order to succeed within the underground economy and generate interest from a forum's user base, including virtual machine detection techniques and user interfaces designed to be user-friendly.

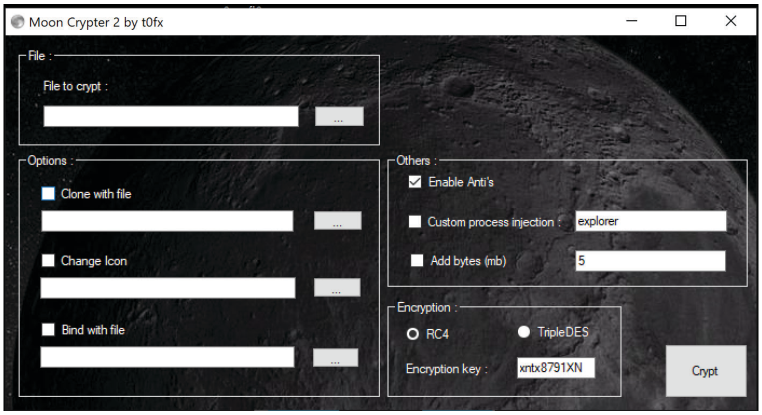
Like many of the other underground commodities outlined in previous Recorded Future research, prices for crypter services remain relatively low, likely to attract a larger audience as well as to cater to interested parties of all skill levels and increase revenue.

For an example of the potential revenue generated by these services, in 2017, Alex Bessell, a 21-year-old man from Liverpool, England appeared in court to face 11 charges of cybercrime offenses and was accused of earning more than $700,000 USD from selling crypters. "AlexTM" openly advertised that he would allow anything to be sold on his website, a common practice for threat actors specializing in services related to crypters or bulletproof hosting infrastructure

Threat Analysis: Crypters

Even freely available and cheap crypter programs include robust traits to evade antivirus software and other forms of detection. They will obfuscate and pack the programs to hide suspect Windows API references, or fill the malware with junk code to frustrate analysts. Despite compression, this often inflates the file size of the malware.

The options for "crypting" are diverse. Many free crypters offer encryption via AES, RC4, and TripleDES with a user-defined key, as well as obfuscation via XOR ciphers.



Moon Crypter 2 by t0fx

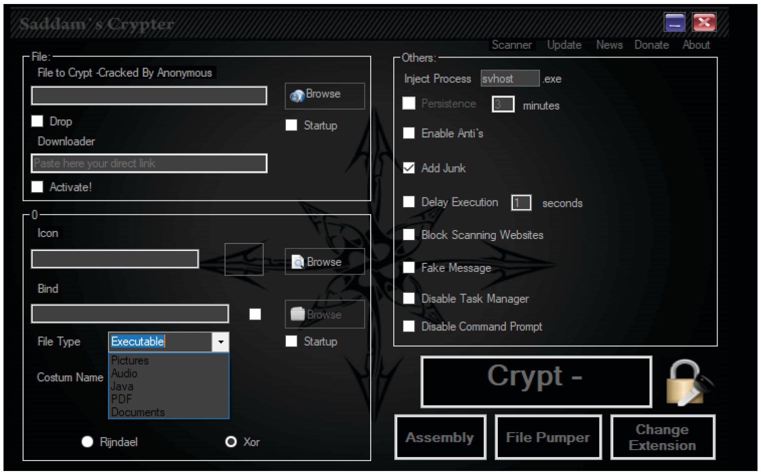
File :
File to crypt :

Options :
□ Clone with file
□ Change Icon
□ Bind with file

Others :
☑ Enable Anti's
□ Custom process injection : explorer
□ Add bytes (mb) 5

Encryption :
○ RC4 ● TripleDES
Encryption key : xntx8791XN

Moon Crypter interface



Saddam's Crypter

File:
File to Crypt -Cracked By Anonymous
□ Drop
Downloader
Paste here your direct link
□ Activate!
□ Startup

0
Icon
Bind
□
File Type: Executable
Pictures
Audio
Java
PDF
Documents
Costum Name
□ Startup
● Rijndael ○ Xor

Others:
Inject Process svhost .exe
□ Persistence 3 minutes
□ Enable Anti's
☑ Add Junk
□ Delay Execution 1 seconds
□ Block Scanning Websites
□ Fake Message
□ Disable Task Manager
□ Disable Command Prompt

Saddam's Crypter interface

Beyond encryption, packing, and obfuscation, many of the crypters offer options to extend the capabilities of the malware being crypted. This includes allowing for process injection, using pop-ups to enable execution to bypass User Account Control (UAC), disabling task managers, and using anti-analysis techniques to thwart debuggers and virtual machines. These anti-analysis techniques hold true in samples pushed through these crypter programs. Furthermore, we found that they often emerge with junk code and we had no clear sight of unpacking code (such as VirtualAlloc API calls). However, both the free tools Moon Crypter and Sadaam's Crypter added less-than-subtle code, such as cleartext references to running WScript for execution or searches for security tools such as ProcessMonitor.

Other crypters helped threat actors deploy additional malware. For instance, Saddam's Crypter allows users to embed the download URL for a second stage, and the crypter would do the heavy lifting to include code in Word Documents or executable files to download and execute additional files.

Mitigation Strategies

- Although crypters are designed to defeat antivirus scanning, other incident response and detection controls may be able to detect the unpacked payload at runtime, like a network intrusion detection system (IDS), endpoint monitoring, netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- The most common attack vector is, and has been, phishing email campaigns containing malicious links and documents with embedded macros. Employees should be given email safety and phishing detection training at regular intervals.
- Due to the targeted aspects of phishing campaigns, alert or block on emails that contain subject lines discussing invoices, human resources, COVID mitigation and response efforts, and termination notifications.
- Given the prevalent malicious use of macros, disable MS Office macros unless necessary for business operations. If for some reason macros are needed, have such policy exceptions approved by IT Security on a case-by-case basis.

Outlook

The market for offering automated and customized loaders and crypters over the last six months has continued to increase, with threat actors offering updated and new variants that are accessible via clearnet websites as well as through purchased services. Given this demand as well as the recently imposed work-from-home measures due to the COVID-19 pandemic, threat actors are likely to continue to use these loader and crypter services to facilitate their criminal activities as they target various victims.