


Multi-Platform SMAUG RaaS Aims To See Off Competitors

 labs.sentinelone.com/multi-platform-smaug-raas-aims-to-see-off-competitors/

Jim Walter



A few years ago public RaaS (Ransomware as a Service) offerings were plentiful. SATAN, Nemesis, Petya, RaaSberry, Shark, Data Keeper...the list goes on. However, the trend, especially in the last year, has been for these services to become increasingly exclusive. NEMTY Revenue & Zeppelin are two prime examples of this.

Still, every now and then we stumble across a fully public service. It gets even more interesting when that service offers a “seamless” experience across OS platforms. Ransomware families with full feature parity across Windows, Linux and macOS do not pop up all that often, which brings us to today’s topic: the SMAUG RaaS (Ransomware as a Service) offering.

SMAUG’s Differentiators

The SMAUG RaaS emerged towards the end of April 2020, and seems to have gained some traction in the following months. SMAUG appears to be a robust and full-service RaaS, with a few tweaks that set it apart from the others.

Criminals who wish to become SMAUG “distributors” will likely be used to the offerings associated with this type of service. The SMAUG operators currently charge a 20% service fee. However, there is also a registration fee which is quite steep when compared to other

“fully-public” services. The current registration fee is .2 BTC, around \$1800 USD at today’s prices.


There are some possible exceptions to getting around the registration fee. On some forums where SMAUG is advertising, the developers state that free memberships (owing only the service fees) will be given to the first five customers with a certain number of posts, and the ability to prove their past work (attacks).



Become Agent

By registering you join a privileged group of cyber criminals wielding the power of SMAUG ransomware. SMAUG ransomware lets you focus on your thing - infecting hosts, while we take care of developing high quality ransomware and maintaining stable infrastructure to automatically receive payments from your victims.

Contact us: smaug_ransomware@protonmail.com

Price 

Registration: 0.2BTC

Service fee: 20%

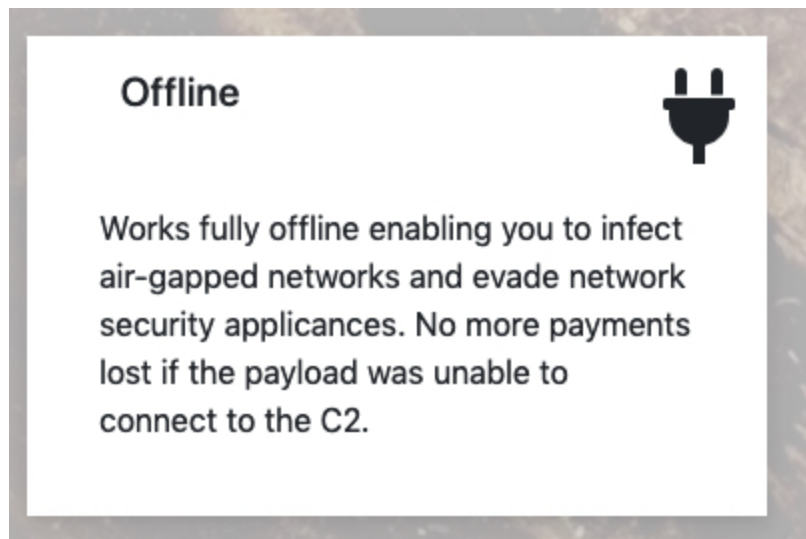
Email

Password

Password again

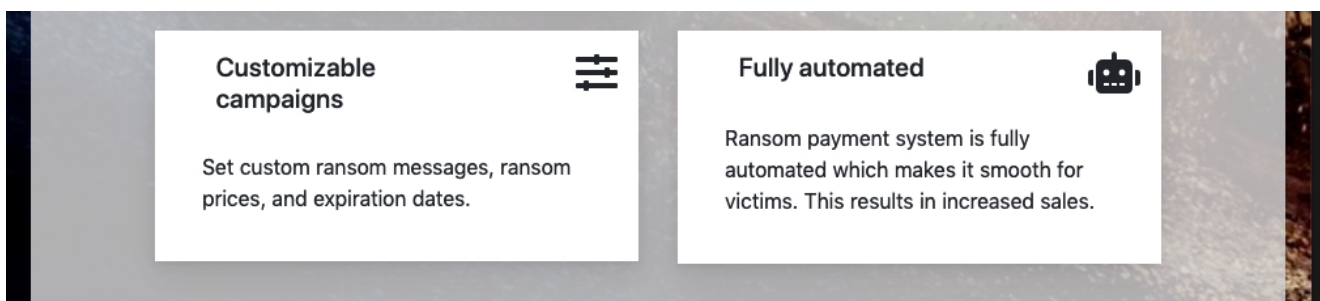
Perhaps the most interesting differentiators are multi-platform support (all 64-bit) and the inclusion of a “Company Mode”, which allows for a single key to apply to an entire body of infected ‘hosts’ (aka a targeted company). If the victim chooses to comply with the attackers, then a single key can be used to decrypt (theoretically) all the encrypted hosts in that environment.

SMAUG also has offline capabilities, meaning that the payload does not have to have any amount of connectivity in order to execute and encrypt.



SMAUG is designed to evade traditional AV products. Along with crypting/obfuscation, the payloads have been developed to have as minimal a footprint as possible.

It should be noted that SMAUG does not appear to include a native crypting/packing feature. Consequently, the developers advise attackers to further obfuscate their payloads. They note the following within the Campaign configuration options of the SMAUG management interface: *“Even though the payload is stealthy it is recommended to use crypting service to ensure the payload is undetectable by antivirus solutions.”*



The operators advertise a fully automated payment system, as well as highly customizable campaigns. This allows attackers to streamline and organize multiple campaigns within the management interface.

Create Campaign

Campaign name	Campaign name
Campaign type	REGULAR
Campaign price (BTC)	1.0
Ransom message	Your files have been encrypted using military grade encryption. They can never be accessed again without buying a decryption key. You can buy the decryption key at http://s1.onion . To access the site you need Tor Browser.
Expiration date	mm/dd/yyyy
Security code	Security code

Create

Most RaaS operators offer a high level of “support” for their affiliates, and this one is no different. SMAUG offers full support for both their customers and victims.

Additional perks

Keep it simple - Just generate the payload using our simple web UI, download the payload, and run it on a victim system. No more obscure and broken builders with tons of dependencies you do not dare to run.

Show the victims you have the keys - Our service automatically decrypts one file per machine for free.

Take care of your victims - Our helpful support staff helps your victims through the decryption process.

Need something special? - Our dynamic development team takes general feature suggestions and incorporates them into the service for free. Features only you require can be discussed.

Customizable Malware, But Mind Your Targets

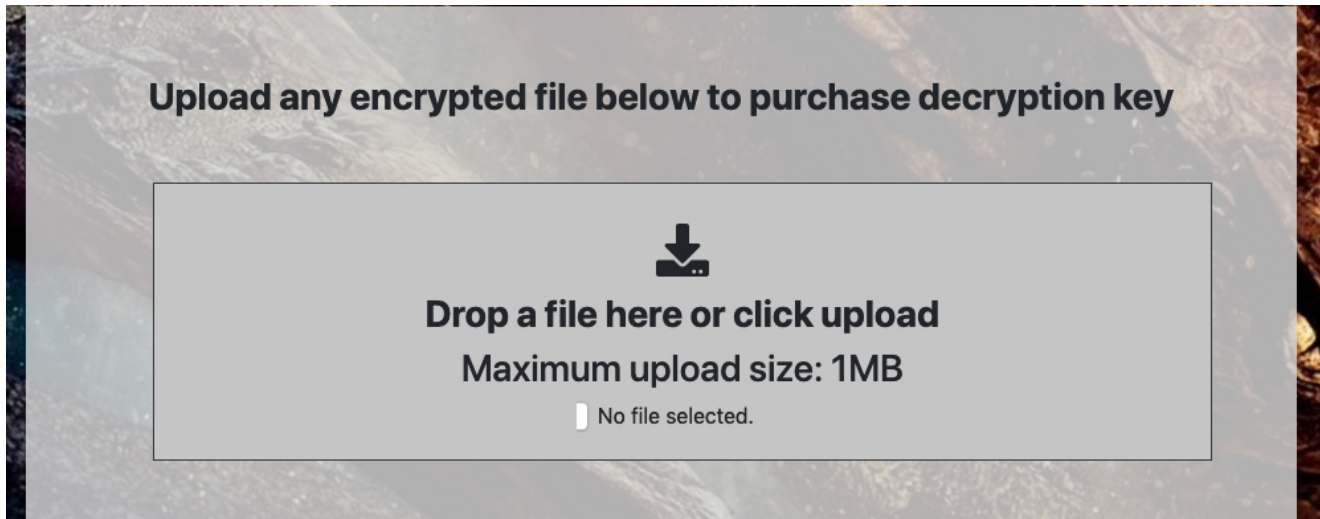
In SMAUG’s service advertisements, they state “*Infecting CIS is forbidden and will result in a ban*” In this context, CIS is the ‘Commonwealth of Independent States’ aka the group of independent countries that were once part of the Soviet Union.

Campaigns created by SMAUG are, as stated, fully customizable, allowing attackers to set their desired price (BTC), deadline/timing constraints, as well as the actual ransom note’s message.

SMAUG-generated malware is designed to execute extremely fast. They tout this as follows:

“The payload utilizes multi-threaded native code which ensures the encryption is done before your victims can react to it.”

Payloads are generated directly in SMAUG's web-based management interface. While many RaaS offerings provide their own offline builder, this can often complicate the process, and lead to issues for the aspiring attackers. SMAUG works around this with their "simple web UI". Victims are able to submit a single file for decryption for free. Beyond that, they must comply with the ransom demands as set in the campaign.



Individual files are encrypted via AES-256. An RSA-2048 public key is used to encrypt the AES encryption key.

Go Payloads

The SMAUG payloads for Windows are obfuscated Go binaries. With that in mind, these payloads begin to bear a resemblance to other similar Ransomware services (ex: [Project Root](#)).

```
crypto/cipher.NewCBCEncrypter
crypto/cipher.(*cbcEncrypter).BlockSize
crypto/cipher.(*cbcEncrypter).CryptBlocks
crypto/aes.encryptBlockGo
crypto/aes.(*aesCipher).Encrypt
crypto/aes.(*aesCipherAsm).Encrypt
crypto/aes.encryptBlockAsm
crypto/aes.(*aesCipherGCM).Encrypt
crypto/rsa.encrypt
crypto/rsa.EncryptOAEP
Lock/internal/pkg/encryption.EncryptFile
Lock/internal/pkg/encryption.pad
Lock/internal/pkg/encryption.padSize
Lock/internal/pkg/encryption.RsaEncrypt
src/Lock/internal/pkg/encryption/rsa.go
src/Lock/internal/pkg/encryption/aes.go
Encrypt
NewCBCEncrypter
```

```
vendor/golang.org/x/net/dns/dnsmessage.Type.String
vendor/golang.org/x/net/dns/dnsmessage.printUint16
vendor/golang.org/x/net/dns/dnsmessage.Type.GoString
vendor/golang.org/x/net/dns/dnsmessage.Class.String
vendor/golang.org/x/net/dns/dnsmessage.Class.GoString
vendor/golang.org/x/net/dns/dnsmessage.RCode.String
vendor/golang.org/x/net/dns/dnsmessage.RCode.GoString
vendor/golang.org/x/net/dns/dnsmessage.printUint32
vendor/golang.org/x/net/dns/dnsmessage.init
vendor/golang.org/x/net/dns/dnsmessage.(*RCode).GoString
vendor/golang.org/x/net/dns/dnsmessage.(*RCode).String
vendor/golang.org/x/net/dns/dnsmessage.(*Type).GoString
vendor/golang.org/x/net/dns/dnsmessage.(*Type).String
vendor/golang.org/x/net/dns/dnsmessage.(*Class).GoString
vendor/golang.org/x/net/dns/dnsmessage.(*Class).String
vendor/golang.org/x/crypto/cryptobyte.init
/usr/local/go/src/vendor/golang.org/x/crypto/cryptobyte/asn1.go
/usr/local/go/src/vendor/golang.org/x/net/dns/dnsmessage/message.go
```

Upon launch the malware will drop a copy of itself into a local driver directory, such as:

```
C:WindowsSysWOW64drivers
C:WindowsSystem32drivers
```

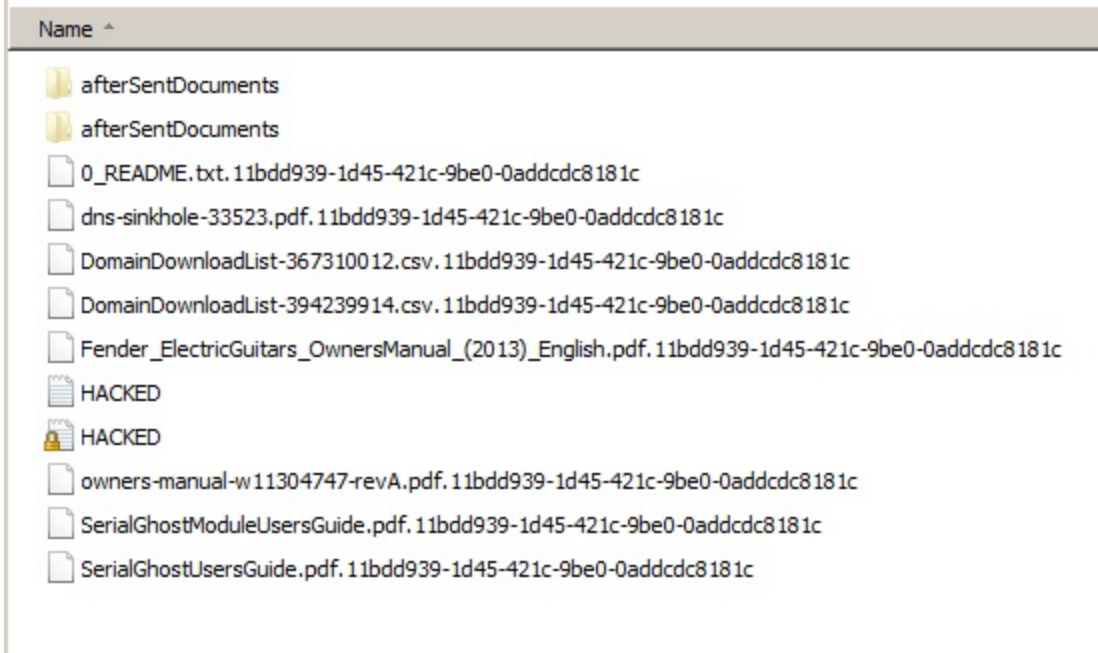
The malware will then attempt to establish persistence via LoadApplnit_DLLs key in the registry. For example,

```
HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWindowsLoadAppInit_DLLs
```

The SMAUG payloads contain additional functionality to gather system information and stored browser credentials. Encryption is achieved via simple AES-256, again similar to Project Root and other Go-based ransomware services. Upon encryption, affected files will have a lengthy extension added (e.g., `11bdd939-1d45-421c-9be0-0addcdc8181c`)

Documents library

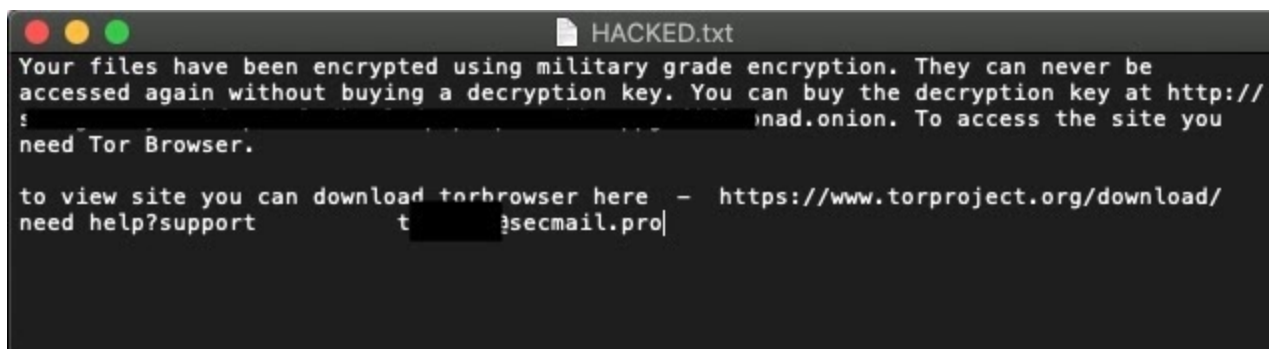
Includes: 2 locations



A ransom note is deposited in all directories containing encrypted files. In our analyzed example, the dropped ransom note was simply named “HACKED.TXT” with the following contents:

“Your files have been encrypted using military grade encryption. They can never be accessed again without buying a decryption key. You can buy the decryption key at [http://\[redacted\].onion](http://[redacted].onion). To access the site you need Tor Browser.

to view site you can download torbrowser here – [https://www.torproject.org/download/need-help?support \[redacted\]@secmail.pro](https://www.torproject.org/download/need-help?support=[redacted]@secmail.pro)”



Victims are instructed, via the ransom note, to visit SMAUG’s onion-based portal for payment instructions and processing.

Upload any encrypted file below to purchase decryption key



Drop a file here or click upload

Maximum upload size: 1MB

No file selected.

Please enter security code

6 9 2 3 a 5 1 c

Please enter security code

submit

Oddly enough, SMAUG appears to have one of the most “helpful” payment (*aka* extortion) portals we have seen. Their walkthroughs (for both victims and affiliates) are very thorough:

Your files have been encrypted using military grade encryption. Many of your files are no longer accessible because of the encryption. The encryption cannot be broken without purchasing the decryption key. You can purchase the decryption key from us using bitcoins.

After you have purchased the decryption key your order will be automatically processed by our system within 10 minutes **after the payment has at least 6 confirmations**. You will receive the key along with a program to decrypt your files. To prove that our decryption key works on your files we will decrypt one of your files for free. **Please upload the file you want decrypted using the form above**. After uploading you will be given further information how to purchase the key.

Depending on the agent that infected your files there might be a deadline for your payment. After the deadline the decryption key for your files is automatically erased from our servers. This means nobody can longer recover your files. Therefore do not waste your time. **Upload one of your encrypted files above to find out how much the decryption key costs and what is the deadline.**

Walkthrough

Here you find information for both victims and agents.

Table of contents

- 1 Victim
 - 1.1 View ransom
 - 1.2 Payment
 - 1.3 Decryption
 - 1.4 Help
 - 1.5 FAQ
- 2 Agent
 - 2.1 Registration
 - 2.2 Campaign creation
 - 2.3 Campaign management
 - 2.4 Withdrawal
 - 2.5 Support
 - 2.6 Change password
 - 2.7 FAQ

Conclusion

Protecting your environment against threats like SMAUG is more critical than ever. In order to prevent loss of data and the consequences of a large-scale data breach, organizations must rely on a modern, well maintained, and properly-tuned and trusted security solution. Prevention is key with these attacks. Even in the event that the encryption/data-loss can be mitigated through decryptors, backups or rollbacks, victims still face the problem of their data being posted publicly. We encourage security teams to analyze and understand the threats and to take swift and appropriate action to prevent incidents occurring in the first place.

Indicators of Compromise

SHA1

929b10f78565660535a07917d144d00b0c117571

SHA256

F2363a355fe226cb2f7f1afa72daecc5edfe1cb0edc1295856fb3f874d941b6d

MITRE ATT&CK

Data Encrypted for Impact [T1486](#)

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547](#)

Exfiltration Over C2 Channel [T1041](#)

Obfuscated Files or Information [T1027](#)

Credentials from Password Stores T1555

Credentials from Password Stores: Credentials from Web Browsers T1555.003

Inhibit System Recovery T1490