Introduction:

Hacking forums often double up as underground marketplaces where cybercriminals buy, rent, and sell all kinds of malicious illegal products, including software, trojans, stealers, exploits, and leaked credentials. Malware-as-a-service has contributed substantially to the growth of ransomware and phishing attacks (among other attack types) in the past year, as they lower the technical barrier to entry for criminals to carry out attacks.

While recently perusing one of these hacking forums during regular research activities, the Zscaler ThreatLabz team came across BlackGuard, a sophisticated stealer, advertised for sale. Blackguard is currently being sold as malware-as-a-service with a lifetime price of $700 and a monthly price of $200.

BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients.

In this blog, we share analysis and screenshots of the techniques this stealer uses to steal information and evade detection using obfuscation, as well as techniques used for anti-debugging.

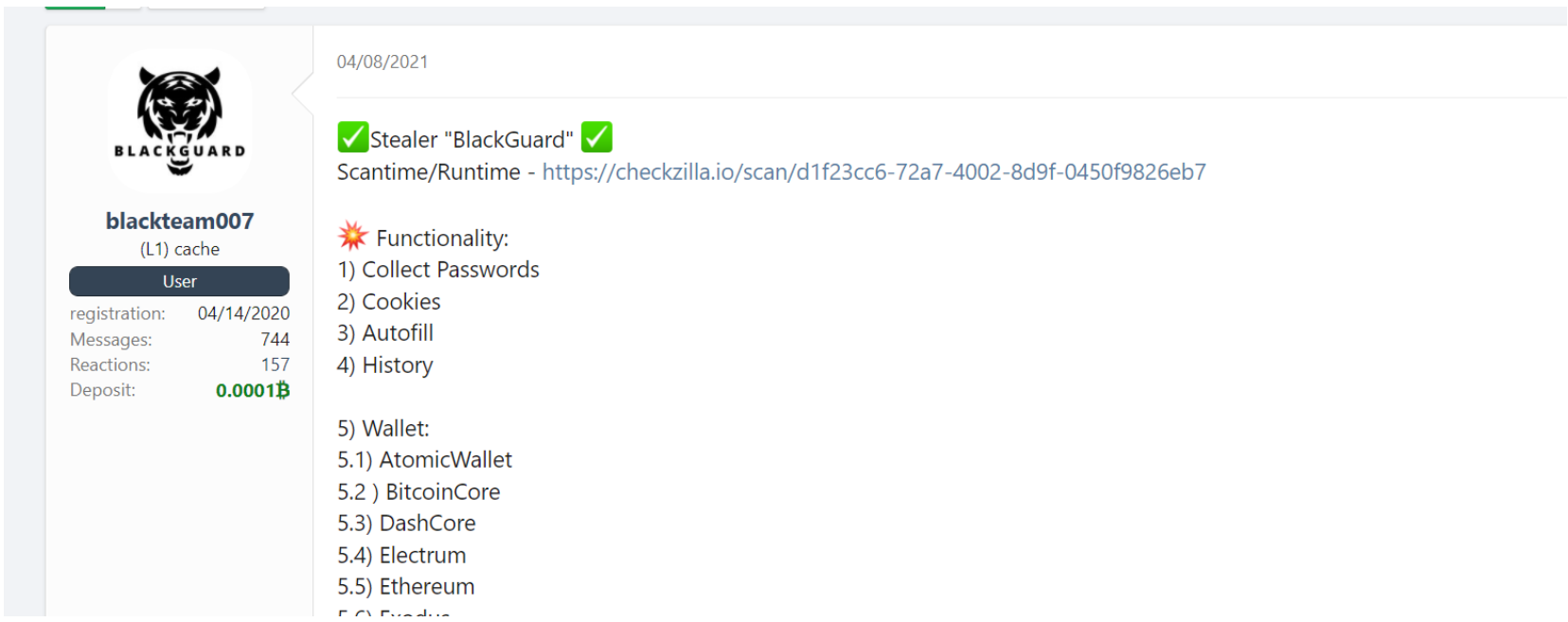

Fig 1. Forum thread promoting the BlackGuard stealer

Technical Analysis:

BlackGuard is a .NET stealer packed with a crypto packer. Currently, it is in active development and has the following capabilities:

Anti-Detection:

Once executed, it checks and kills the processes related to antivirus and sandbox as shown in the figure below.

```
if (Class52.smethod_1())
{
    Process.GetCurrentProcess().Kill();
}
```

Locals

Name	Value	Type
<PrivateImplementationDetails>{685EF87B-40D6-445A-A5D9-43...	"U2JpZURsbC5kbGw="	string
ns0.Class52.b64_decode returned	"SbieDll.dll"	string
<PrivateImplementationDetails>{685EF87B-40D6-445A-A5D9-43...	"U3hJbi5kbGw="	string
ns0.Class52.b64_decode returned	"SxIn.dll"	string
<PrivateImplementationDetails>{685EF87B-40D6-445A-A5D9-43...	"U2YyLmRsbA=="	string
ns0.Class52.b64_decode returned	"Sf2.dll"	string
<PrivateImplementationDetails>{685EF87B-40D6-445A-A5D9-43...	"c254aGsuZGxs"	string
ns0.Class52.b64_decode returned	"snxhk.dll"	string
<PrivateImplementationDetails>{685EF87B-40D6-445A-A5D9-43...	"Y21kdnJ0MzIuZGxs"	string
ns0.Class52.b64_decode returned	"cmdvrt32.dll"	string

Fig 2. BlackGuard detects antivirus processes

String Obfuscation:

The stealer contains a hardcoded array of bytes which is decoded in runtime to ASCII strings followed by base64 decoding. This allows it to bypass antivirus and string-based detection.

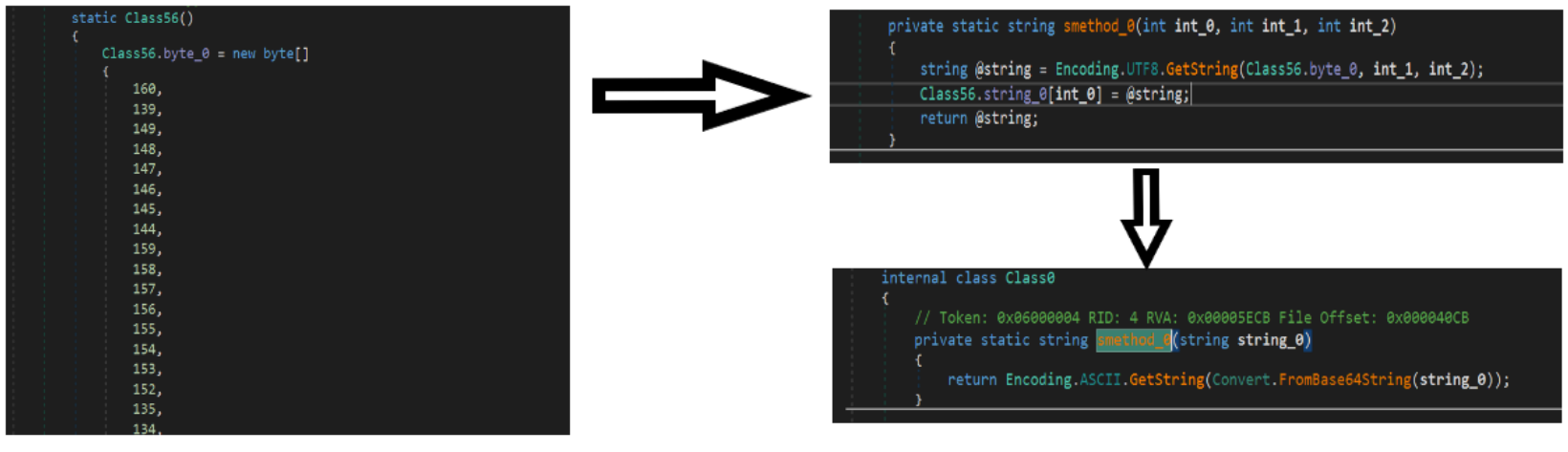

Fig 3. String decryption technique

Anti-CIS:

BlackGuard checks for the infected device country by sending a request to “http://ipwhois.app/xml/” and exits itself if the device is located in the Commonwealth of Independent States (CIS).

Fig 4. Whitelist CIS

Anti-Debug:

BlackGuard uses user32!BlockInput() which can block all mouse and keyboard events in order to disrupt attempts at debugging.

Fig 5. Anti-debugging technique

Stealing Function:

After all the checks are completed, the stealer function gets called which collects information from various browsers, software, and hardcoded directories, as shown in the screenshot below.

Fig 6. Stealer code

Fig 7. Features Posted on forum

Browsers:

BlackGuard steals credentials from Chrome- and Gecko-based browsers using the static path. It has the capability to steal history, passwords, autofill information, and downloads.

Fig 8. Browser stealing function

Cryptocurrency Wallets:

BlackGuard also supports the stealing of wallets and other sensitive files related to crypto wallet applications. It targets sensitive data in files such as wallet.dat that contain the address, the private key to access this address, and other data. The stealer checks for the default wallet file location in AppData and copies it to the working folder.

Fig 9. Crypto wallet stealing function

Crypto Extensions:

This stealer also targets crypto wallet extensions installed in Chrome and Edge with hardcoded extension IDs as shown in the figure below.

Fig 10. Crypto extensions stealing function

C2 Exfiltration:

After collecting the information, BlackGuard creates a .zip of all the files and sends it to the C2 server through a POST request along with the system information like Hardware ID and country as shown in the figure below.

Fig 11. C2 Exfiltration code snippet

Fig 12. Traffic capture of exfiltration

Fig 13. Panel screenshot

Targeted Applications:

Browsers:

Chrome, Opera, Firefox, MapleStudio, Iridium, 7Star, CentBrowser, Chedot, Vivaldi, Kometa, Elements Browser, Epic Privacy Browser, uCozMedia, Coowon, liebao, QIP Surf, Orbitum, Comodo, Amigo, Torch, Comodo, 360Browser, Maxthon3, K-Melon, Sputnik, Nichrome, CocCoc, Uran, Chromodo, Edge, BraveSoftware.

Crypto Wallets:

AtomicWallet, BitcoinCore, DashCore, Electrum, Ethereum, Exodus, LitecoinCore, Monero, Jaxx, Zcash, Solar, Zap, AtomicDEX, Binance, Frame, TokenPocket, Wassabi.

Crypto Wallet Extensions:

Binance, coin98, Phantom, Mobox, XinPay, Math10, Metamask, BitApp, Guildwallet, iconx, Sollet, Slope Wallet, Starcoin, Swash, Finnie, KEPLR, Crocobit, OXYGEN, Nifty, Liquality, Auvitas wallet, Math wallet, MTV wallet, Rabet wallet, Ronin wallet, Yoroi wallet, ZilPay wallet, Exodus, Terra Station, Jaxx.

Email Clients:

Outlook

Other Applications:

NordVPN, OpenVPN, ProtonVpn, Totalcomander, Filezilla, WinSCP, Steam

Messengers:

Telegram, Signal, Tox, Element, Pidgin, Discord

Conclusion:

While applications of BlackGuard are not as broad as other stealers, BlackGuard is a growing threat as it continues to be improved and is developing a strong reputation in the underground community.

To combat against BlackGuard and similar credential theft malware, we recommend that security teams inspect all traffic and use malware prevention tools that include both antivirus (for known threats) and sandboxing capabilities (for unknown threats). We also recommend training end users on the following:

1. Don’t use the same passwords for all the services and replace them on a regular cadence.
2. Use multi-factor authentication where applicable.
3. Avoid visiting unknown sites.
4. Avoid opening suspicious unknown files.

IOCs:

Hashes:

4d66b5a09f4e500e7df0794552829c925a5728ad0acd9e68ec020e138abe80ac

c98e24c174130bba4836e08d24170866aa7128d62d3e2b25f3bc8562fdc74a66

7f2542ed2768a8bd5f6054eaf3c5f75cb4f77c0c8e887e58b613cb43d9dd9c13

f2d25cb96d3411e4696f8f5401cb8f1af0d83bf3c6b69f511f1a694b1a86b74d

bbc8ac47d3051fbab328d4a8a4c1c8819707ac045ab6ac94b1997dac59be2ece

f47db48129530cf19f3c42f0c9f38ce1915f403469483661999dc2b19e12650b

ead17dee70549740a4e649a647516c140d303f507e0c42ac4b6856e6a4ff9e14

1ee88a8f680ffd175943e465bf85e003e1ae7d90a0b677b785c7be8ded481392

71edf6e4460d3eaf5f385610004cfd68d1a08b753d3991c6a64ca61beb4c673a

e08d69b8256bcea27032d1faf574f47d5412b6da6565dbe52c968ccecea1cd5d

Domains:

win.mirtonewbacker.com

umpulumpu.ru

greenblguard.shop

onetwostep.at

Zscaler coverage:

We have ensured coverage for the payloads seen in these attacks via advanced threat signatures as well as our advanced cloud sandbox.

Advanced Threat Protection:

Win32.PWS.Blackguard

Advanced Cloud Sandbox:

Fig 14. Zscaler sandbox detection

- Security Research
- Insights and Research
-

Authors

Mitesh Wani

Kaivalya Khursale

Recommended for You

Conti Ransomware Attacks Persist With an Updated Version Despite Leaks

Lapsus$ Attack on Okta: How to Evaluate the Impact to your Organization

Midas Ransomware : Tracing the Evolution of Thanos Ransomware Variants

Domain Fronting, Abuse and Hiding