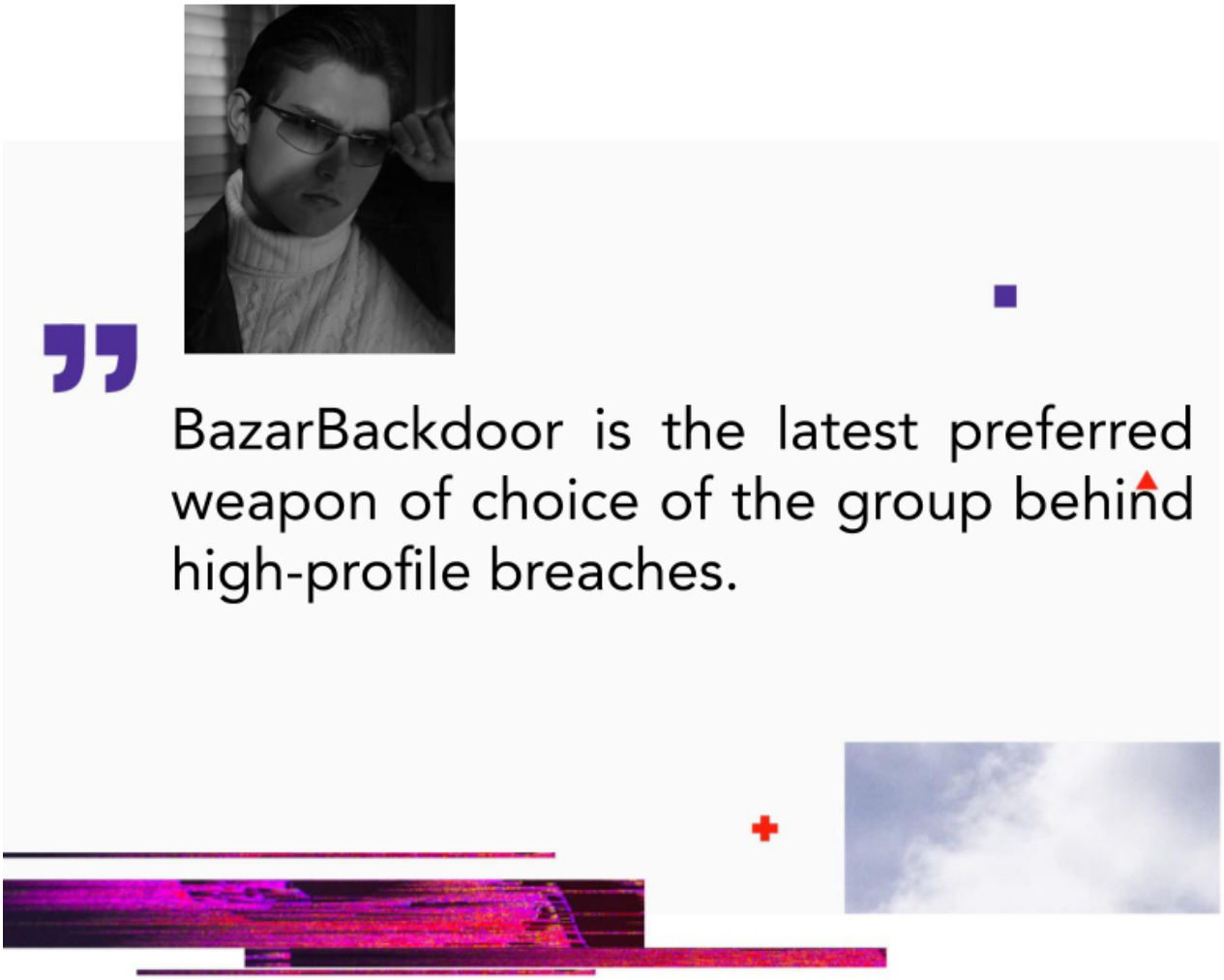
"Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon

advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon

AdvIntel October 12, 2020

- Oct 12, 2020
-
- 7 min read

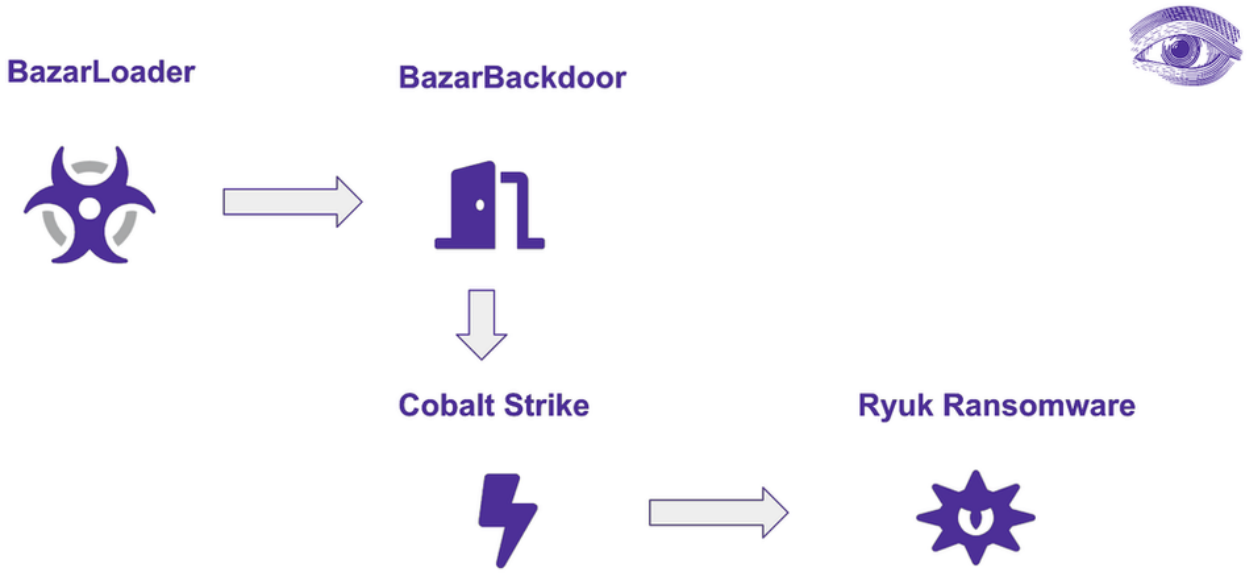
By Roman Marshanski & Vitali Kremez



Key Points

- BazarBackdoor is the newer preferred stealthy covert malware leveraged for high-value targets part of the **TrickBot** group toolkit arsenal. It consists of two components: a loader and a backdoor.

- The Bazar malware group pursues stealthiness via malware signing and only initially loading minimal malware functionality. Such an approach improves the malware chance of long-term persistence inside the most secure networks.
- Just like professional penetration testers, the crime group behind the **BazarBackdoor** employs legitimate penetration software kit **Cobalt Strike** for post-exploitation for enumerating and harvesting credentials for network hosts and active directory, uploading third-party software like "**Lasagne**" and "**BloodHound**" as well pivoting inside the network domain executing **Ryuk** ransomware.
- **Advanced Intelligence** experts include the relevant defense and hunting mechanisms such as the YARA signature for BazarBackdoor detection.



BazarBackdoor is the newer preferred stealthy covert malware leveraged for high-value targets part of the TrickBot group toolkit arsenal. It consists of two components: a loader and a backdoor. [1]

Loaders are an essential part of any cybercrime campaign. They start the infection chain by distributing the payload. In essence, they deploy and execute the backdoor from the command-and-control (C2) layer and plant it on the victim's machine. But the reality is far more complicated than that. After all, loaders and backdoors must be able to evade detection by various security mechanisms. And that is where the malware developers' focus on malware stealthiness comes into play.

Just like professional penetration testers, the crime group behind the BazarBackdoor employs legitimate penetration software kit Cobalt Strike for post-exploitation for enumerating and harvesting credentials for network hosts and active directory, uploading third-party software like Lasagne and BloodHound as well pivoting inside the network domain executing **Ryuk** ransomware.

Malware Stealthiness as Key Approach

As we learned from our multiple incident response cases, the BazarLoader's strength lies in its stealthy core component and obfuscation capability. The malware's goal is to plant on the high-value targets and reach the server currently via the proxy and the domain generation algorithm on the **EmerDNS** domain protocol, searching for .bazar domains and resolving the server via the XOR function of the response IP address.

The malware aimed to be stealthy and only load more advanced functionality via third-party components such as Cobalt Strike beacons. Such stealthiness allows the crime group to maintain persistency on the host even if the third-party software gets detected by anti-virus software.

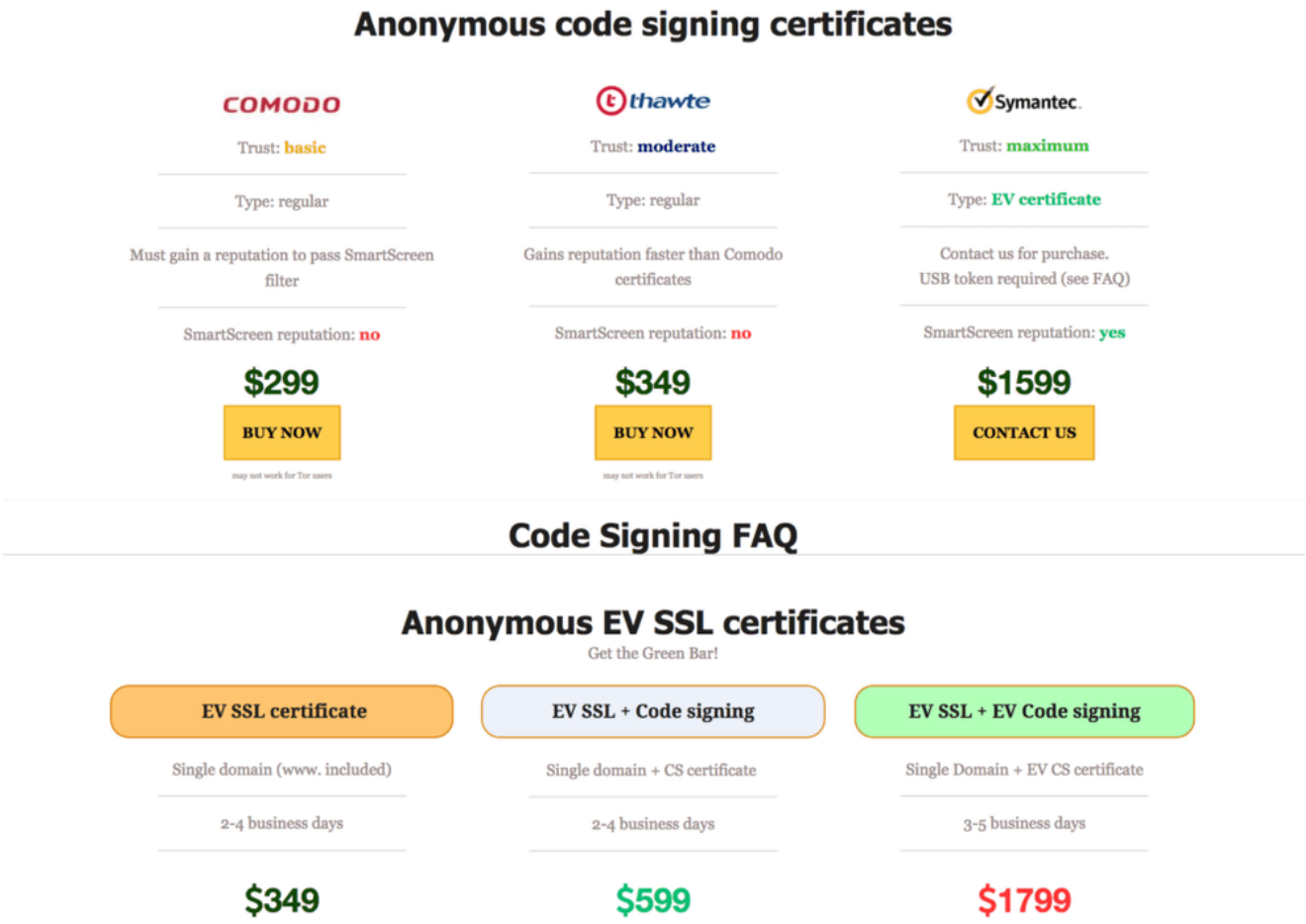
BazarLoader: Malware Signing

The group behind also takes advantage of certificate signing, evading particular anti-virus and other software products.

The use of certificate authorities is widespread in the cybercriminal world. Historically it was frequently a domain of advanced persistent threat groups (APTs). BazarLoader demonstrates that alarming trend. The usage of certificates exploits the trust of certificate authorities by using both new and revoked certificates.

While it may be slightly comforting to know that BazarLoader operators use revoked certificates up to six months after their expiration, they can easily purchase new ones. They can buy original code signing certificates for anywhere between $295 USD and $1,799 USD.

The screenshot of a product listing by a threat actor selling these certificates illustrates this below.



It is especially alarming that these certificates available to any cybercriminal are legitimate. The threat actor uses real corporations' information to register these certificates with major, widely trusted certificate authorities. Furthermore, as can be seen from the above screenshot, even fully authenticated domains with EV SSL encryption are available for the cybercriminals. Such availability underscores the new reality in which even the most secure certificates should never be blindly trusted. Caution must be exercised every step of the way.

The use of code signing certificates allows Bazar operators to decrease detection rates significantly. According to the threat actor selling these certificates, their use reduces detection rates by 30 to 50 percent. Considering the profit margins of Bazar operators, it is highly likely they will continue buying these certificates. For them, these certificates are an investment with a high return of investment.

BazarLoader: Use Of The Blockchain Technology

The ingenious use of blockchain is another smart investment decision by Bazar operators. This has cost them even less than the code signing certificates. The price of a blockchain-based, takedown resistant domain called the EmerDNS domain is less than 1 Emercoin per one year. This is less than one US cent.

It should be mentioned, though, that prominent companies use Emercoin blockchain technology. Deloitte is one example as well as the US government regulation integrity project. So once again, Bazar operators display an ability to use legitimate services for nefarious ends.

In particular, they use EmerDNS (.bazar) domains for connections with C2 servers. Because these domains use blockchain technology, law enforcement, or security, researchers' discovery does not threaten the cybercriminals' operation. Neither legal takedown nor sinkhole can disrupt these domains. So the creative use of EmerDNS (.bazar) domains is the reason this loader is called "BazarLoader."

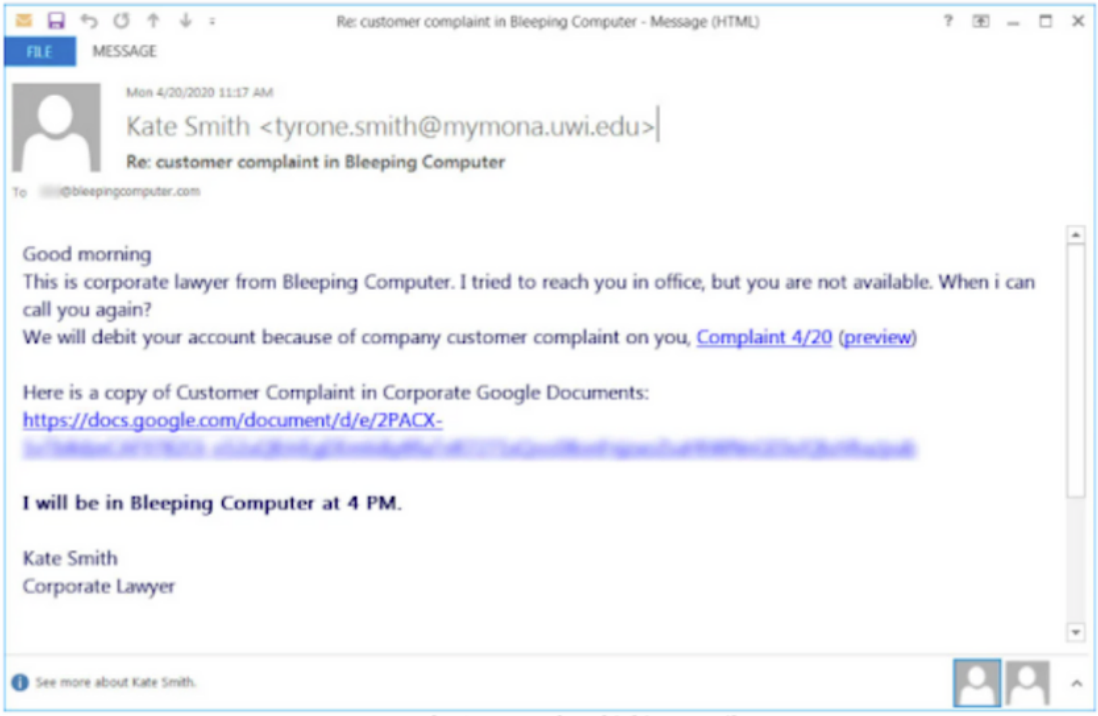
More recently, the group introduced the domain generation algorithm (DGA) in the EmerDNS network. While the novelty claim appeared to be impressive, it was discovered that the algorithm was flawed. [2] The algorithm provided an alternative server communication channel creating a massive number of name combinations.

The Bazar Malware Infection Chain

The above-mentioned usage of legitimate services by Bazar malware operators is just the tip of the iceberg. They also used legitimate file-sharing services for malware spreading.

While phishing emails are commonplace in the cybercriminal campaigns, as about 91 percent of cyberattacks start with a phishing email, their particular use by Bazar malware operators is more sophisticated than usual. Once again, their tendency to turn legitimate

organizations into unwitting accomplices is on full display, as they use a legitimate and widely used **SendGrid** email marketing platform to send out their phishing emails.



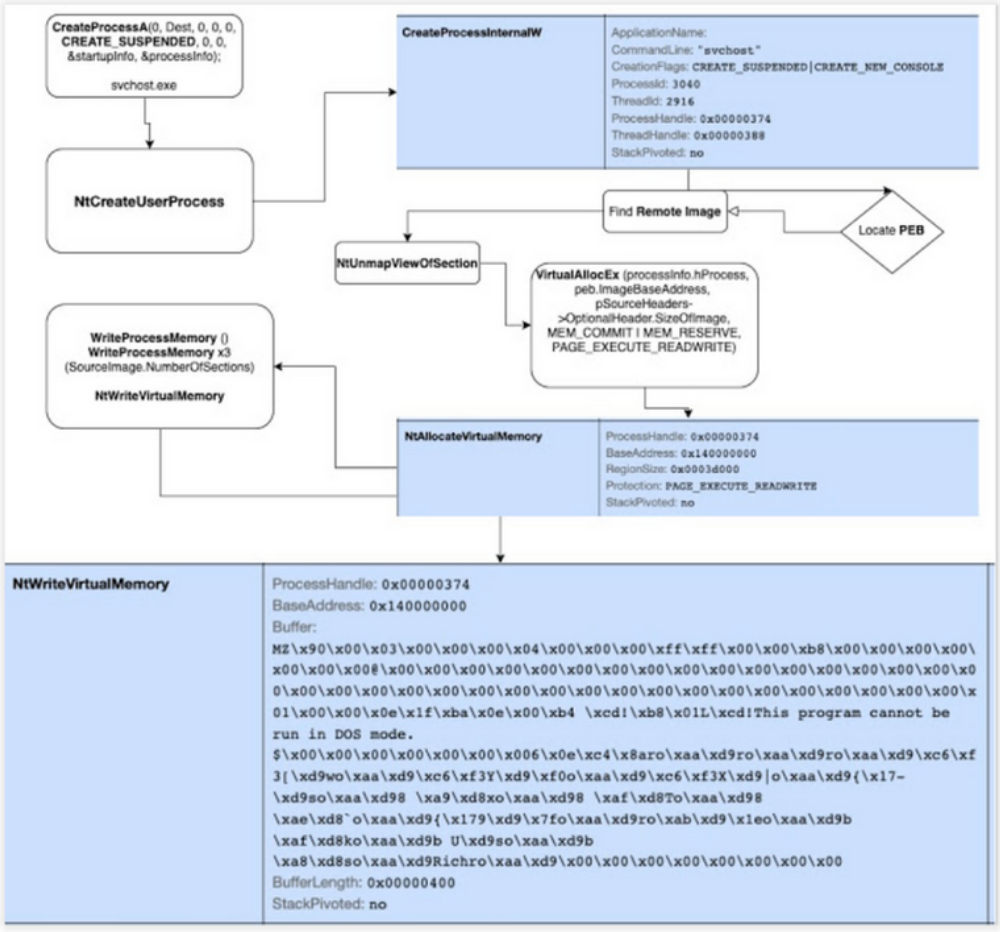
Example BazarLoader phishing email

After the user has clicked on the phishing email link and landed on the decoy preview page, the page tries to trick the user into downloading malicious dual-extension executable files (such as PreviewReport.DOC.exe) by saying that the document preview is unavailable. These malicious dual-extension executable files are the BazarLoader files signed with certificates.

After a series of these deobfuscation processes, the encrypted BazarBackdoor is downloaded and decrypted. After this, the portable executable file header is validated for decryption. At that point, the infection chain moves to its final stage during which the host is compromised.

II. BazarLoader: Process Hollowing Methodology

The malware utilizes the process hollowing injection approach injecting the core backdoor into svchost.exe via the following sequence *CreateProcessA(0, pDestCmdLine, 0, 0, 0, CREATE_SUSPENDED, 0, 0, &startupInfo, &processInfo) -> Find PEB -> Locate Remote Image NtUnmapViewOfSection -> VirtualAllocEx -> VirtualAllocEx(processInfo.hProcess, peb.ImageBaseAddress, ...,MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE) -> WriteProcessMemory () -> WriteProcessMemory (SourceImage.NumberOfSections)*



The loader performs process hollowing via two known methods such as process hollowing and process doppelganging. It injects malicious code into one of the following processes: cmd, explorer, and svchost. Then it executes its own code in the address space of one of them. Since the execution is masked under a legitimate process, the loader often evades some anti-virus detection.

Eventually, a scheduled task with the name such as "StartAd - Ad" is created, the loader writes itself into the Windows registry, and creates autorun entries. Because of this, whenever someone logs on to the system, the loader is able to run. And the loader is protected from discovery in another way: the author of the scheduled task is set as Adobe. So once again, Bazar malware operators display some use of deception.

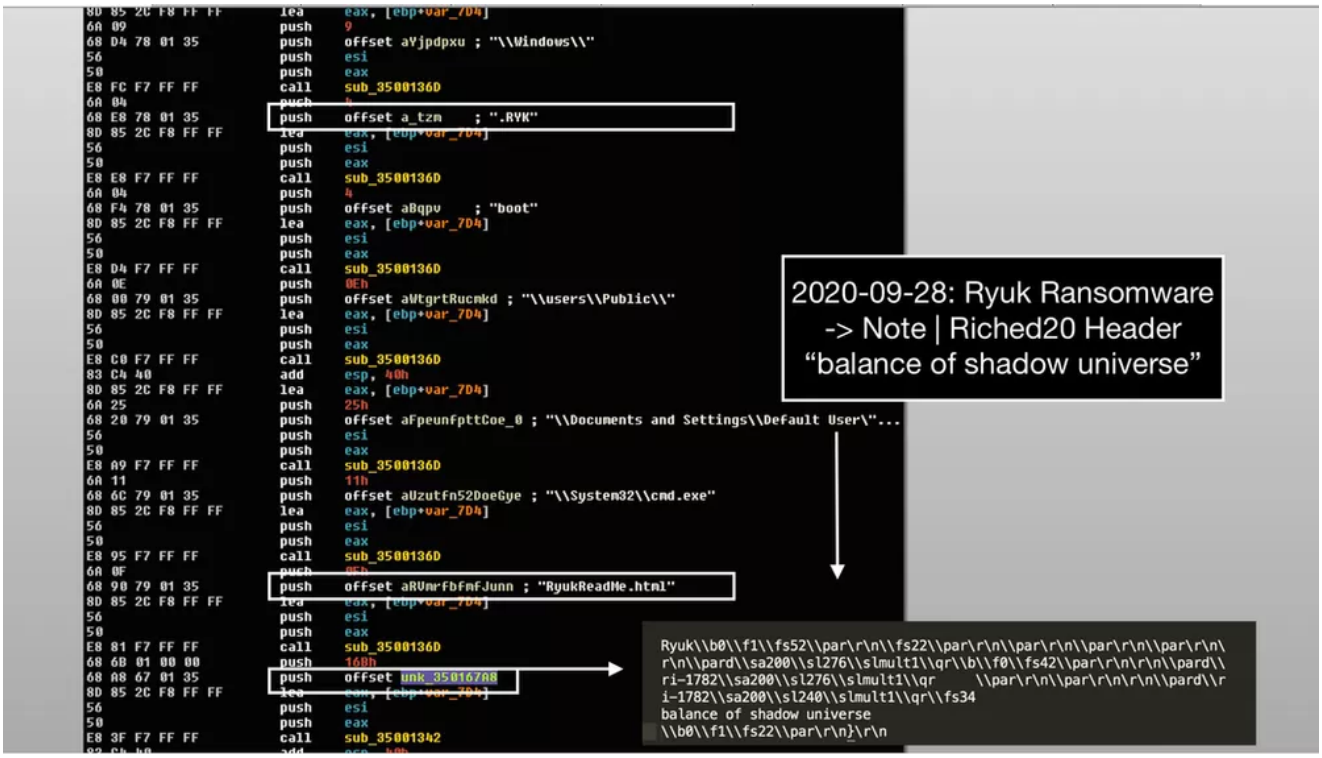
From BazarBackdoor to Cobalt Strike Penetration Software Kit

One of the malware operation's notable components is to download and execute the Cobalt Strike beacons to further access once inside the targeted networks.

Just like professional penetration testers, the crime group behind the BazarBackdoor employs legitimate penetration software kit Cobalt Strike for post-exploitation for enumerating and harvesting credentials for network hosts and active directory, uploading third-party software like Lasagne and BloodHound as well pivoting inside the network domain executing Ryuk ransomware.

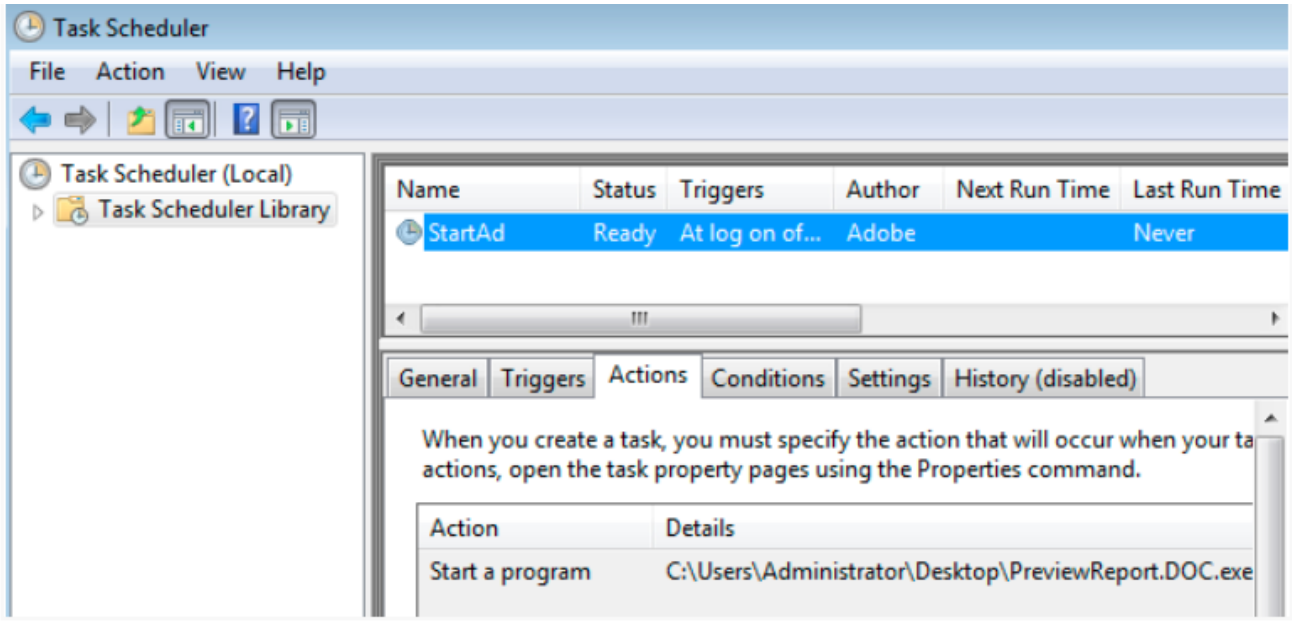
Ryuk Ransomware: BazarBackdoor's Ransomware of Choice

The group behind the malware is also largely responsible for the significant increase of the Ryuk ransomware lately impacting high-profile organizations all over the world.



In The Art of War, Chinese military strategist Sun Tzu wrote that all warfare is based on deception. If so, then Bazar malware operators have turned cybercrime into an art form hunting for high-value targets and combining the use of legitimate services and its simplicity into one arcane web of deception.

Prevention



That indicator of compromise is a scheduled task with the name "StartAd – Ad".

Additionally, watch out for dual-extension executable files (such as PreviewReport.DOC.exe).

Users should be careful not to trust revoked certificates. In particular, be on the lookout for the following revoked certificates used by BazarLoader:

1. VITA-DE d.o.o.
2. VB CORPORATE PTY. LTD.
3. VAS CO PTY LTD
4. THE FLOWER FACTORY S.R.L.

5. SLIM DOG GROUP SP Z O O
6. BlueMarble GmbH
7. PLAN CORP PTY LTD
8. PEKARNA TINA d.o.o.
9. PAMMA DE d.o.o.
10. LIT-DAN UKIS UAB
11. James LTH d.o.o.
12. FLORAL
13. D Bacte Ltd
14. Company Megacom SP Z O O
15. Cebola Limited.

Indicators of Compromise:

```
SHA256: 8c99069bcb559bf7d9606af7ba1538cc8bacd79b4f3846f7487ec3b5179ef9d5
SHA256: d8576fba423360297b0661833a0e06564230c2079db214dc6830c648e5193e51
SHA256: 609fef55693698a2bc7695a4bdc574cfb45b590bde4f4291f8d99bc7f25e266a
SHA256: ca833b3820cff853dc84eb98bf8910249a80a28ed2a7e1da2cc13937df1b39d4
SHA256: bad9f0b937bc7a74cd5657127e7d1707ce024ccb5434044ef305dffd4307f29b
SHA256: 2a7964c5d7268f4b320e91ad133654d75edca3c15f9e5c76dee7bf68634b933f
SHA256: f54cec2b04daafb0a1d612ef84913a1d03ef61d7de8b4c144414378c4415ac09
```

Yara Signature

```
rule crime_win64_backdoor_bazarbackdoor1 {

meta:
 description = "Detects BazarBackdoor injected 64-bit malware"
 author = "@VK_Intel"
 reference = "https://twitter.com/pancak3lullz/status/1252303608747565057"
 tlp = "white"
 date = "2020-04-24"

strings:
 $str1 = "%id%"
 $str2 = "%d"

 $start = { 48 ?? ?? ?? ?? 57 48 83 ec 30 b9 01 00 00 00 e8 ?? ?? ?? ?? 84 c0 0f ??
?? ?? ?? ?? 40 32 ff 40 ?? ?? ?? ?? e8 ?? ?? ?? ?? 8a d8 8b ?? ?? ?? ?? ?? 83 f9 01
0f ?? ?? ?? ?? ?? 85 c9 75 ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48
?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? 85 c0 74 ?? b8 ff 00 00 00 e9 ?? ?? ?? ?? 48 ?? ??
?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? eb ??
40 b7 01 40 ?? ?? ?? ?? 8a cb e8 ?? ?? ?? ?? e8 ?? ?? ?? ?? 48 8b d8 48 ?? ?? ?? 74
??}
 $server = {40 53 48 83 ec 20 48 8b d9 e8 ?? ?? ?? ?? 85 c0 75 ?? 0f ?? ?? ?? ?? ??
?? 66 83 f8 50 74 ?? b9 bb 01 00 00 66 3b c1 74 ?? a8 01 74 ?? 48 8b cb e8 ?? ?? ??
?? 84 c0 75 ?? 48 8b cb e8 ?? ?? ?? ?? b8 f6 ff ff ff eb ?? 33 c0 48 83 c4 20 5b c3}

condition:
 ( uint16(0) == 0x5a4d and ( 3 of them ) ) or ( all of them )

}
```

Mitre ATT&CK Framework:

- T1093 - Process Hollowing
- Signature - TransactedHollowing
- T1055 - Process Injection
- Signature - InjectionInterProcess

Source:

[1] https://www.vkremez.com/2020/04/lets-learn-trickbot-bazarbackdoor.html

[2] https://johannesbader.ch/blog/the-buggy-dga-of-bazarbackdoor/

[3] https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/

Roman Marshanski *investigates and researches underground and* malware *threats at* ***Advanced Intelligence LLC****. He is also the founder of a popular humor website* ***Humoropedia****. Roman focuses on developing websites and implementing security mechanisms. As a result of his website development career, he became interested in cybersecurity, earned a cybersecurity certification, and pursues a career in this field. He* ***fell in love with malware*** *at Advanced Intelligence LLC. Fascinated by malware's innovative and intricate ways, Roman intends to continue his love affair with the most sophisticated and elite malware developments.*

Vitali Kremez *is the Chairman and CEO of Advanced Intelligence, LLC.*