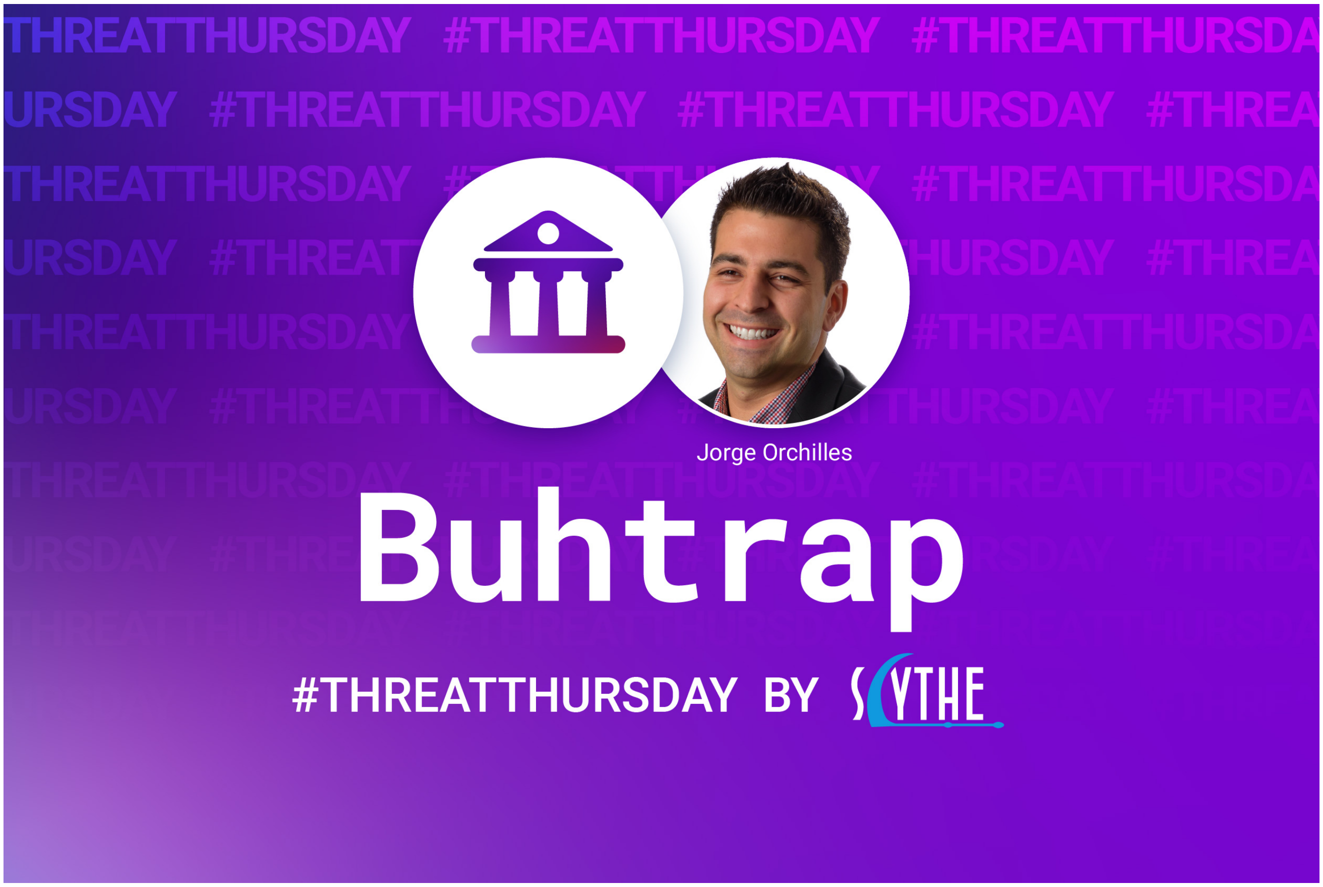
#ThreatThursday - Buhtrap

scythe.io/library/threatthursday-buhtrap

<< All Posts

Jorge Orchilles

June 11, 2020



In this #ThreatThursday we will be looking at Buhtrap, a criminal team attacking financial institutions. We are presenting new concepts this week such as consuming Cyber Threat Intelligence that has not been mapped or tracked on MITRE ATT&CK website and explaining the concept of Short and Long Haul C2.

No MITRE ATT&CK Page for Adversary?

If you read our first #ThreatThursday on APT19, you learned to use the MITRE ATT&CK site and ATT&CK Navigator to extract the adversary tactics, techniques, and procedures (TTPs) to create an adversary emulation plan. Searching for this week's threat actor, Buhtrap, will not yield any results. We will have to dig deeper for Cyber Threat Intelligence and extract the TTPs manually.

Acquire Cyber Threat Intelligence

Google search is a great way to start learning about this threat actor. We found a number of sources:

- https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
- https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/
- https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

Buhtrap Threat Profile

Reading through the sources above (feel free to read other sources) we can extract the TTPs and create a Threat Profile for Buhtrap:

Tactic	Description
Description	Buhtrap group is a criminal team evolved from attacks against bank clients to attacks directly targeting financial institutions. At the moment, the group is known to target Russian and Ukrainian banks
Objective	Financial gain with over 1.8 billion rubles
Command and Control	Commonly Used Port (T1043) - TCP 443 Standard Application Layer Protocol (T1071) - HTTPS Custom Command and Control Protocol (T1094) - DNS Tunnelling
Initial Access	Spearphishing Link (T1192)
Execution	User Execution (T1204) Command-Line Interface (T1059)
Defense Evasion	Code Signing (T1116) Deobfuscate/Decode Files or Information (T1140)
Discovery	File and Directory Discovery (T1083) Network Share Discovery (T1135)
Persistence	Scheduled Task (T1053)
Credential Access	Input Capture (T1056) Clipboard Data (T1115)

Exfiltration	Automated Exfiltration (T1020)
	Data Encrypted (T1022)
	Exfiltration Over Command and Control Channel (T1041)
	Remote File Copy (T1105)

Table 1

Command and Control

You will notice Buhtrap leverages multiple Command and Control (C2) channels. This is common for threat actors and Red Teams performing adversary emulation. We can divide C2 channels in short and long haul. Short haul is for performing actions and receiving results quickly. For example, HTTP beacons at a short interval (seconds) so that interaction is efficient. Long-haul C2 is for maintaining access so operations can be stealthier and maintain persistence; it should be slow and fly under the radar.

Short Haul C2

Short Haul C2 channels are used for quicker interaction with the target systems and performing MITRE ATT&CK tactics like Discover, Privilege Escalation, and Exfiltration. Since short haul C2 is used for a number of TTPs, the risk of getting caught is much higher and the C2 channel may be lost or blocked (burned). Common short haul C2 channels are direct TCP connections, HTTP, HTTPS, HTTP2, HTTP3, and SMB.

Long Haul C2

Long Haul C2 channels are much slower and should be used to recuperate short haul C2s that may have been caught or blocked by the blue team. For example, your short haul uses HTTPS to unicorn.scythedemo.com and it gets blocked by the SOC. Your DNS, long haul C2, that goes to another IP or domain does not get blocked. You would use the DNS C2 to launch a new agent connecting to a non-blocked HTTPS domain. Long haul channels should be configured to beacon out much less frequently (once a day, once a week). Long-Haul channels should be strictly used to regain short haul channels so you do not risk losing all access to the target environment. Common long haul channels are DNS, DoH, ICMP, and steganography channels. This does not mean you cannot or should not use much slower beacons over other channels as long haul either. It all depends on the objectives and what is being tested.

Adversary Emulation Plan

Given we have to set up two C2 channels, we have created and shared two adversary emulation plans on our Community Threats Github for Buhtrap. This will require two campaigns in SCYTHE and therefore should be separated in our plan.

HTTPS

Most of the TTPs performed by Buhtrap will be performed via the short haul C2: Buhtrap-HTTPS This adversary emulation plans performs the following automatically with SCYTHE:

- Commonly Used Port (T1043) - TCP 443
- Standard Application Layer Protocol (T1071) - HTTPS
- Input Capture (T1056) - starts right away to begin capture
- Screen Capture (T1113)
- Clipboard Data (T1115)
- File and Directory Discovery (T1083)
- Network Share Discovery (T1135)
- System Owner/User Discover (T1033)

Once that is complete, the next steps must be done manually as automating persistence will result in automatically emulating the TTP over and over:

- Start DNS campaign - see DNS section
- Deploy payload for long haul C2 over DNS

- Move .DLL to virtual file system

- loader --load downloader

- downloader --src VFS:/users/BUILTIN/scythe/DNS_scythe_client32.dll --dest C:\Users\<user>\DNS_scythe_client32.dll

Establish persistence with Scheduled Task (T1053) and Rundll32 (T1085)

- schtasks /create /tn DNS /sc ONLOGON /tr "cmd.exe /k rundll32.exe C:\Users\<user>\DNS_scythe_client32.dll,PlatformClientMain"

DNS

The adversary emulation plan for the DNS campaign is very basic as we just need connectivity to lay dormant and check in very infrequently: Buhtrap-DNS Once imported it is very important to change the parameters and ensure the DNS relay is functioning properly.

Emulating Buhtrap

With an adversary emulation plan, it is time to set up the campaign and emulate the TTPs. Please watch our video to see how we emulate Buhtrap with SCYTHE:

Defending against Buhtrap

Buhtrap uses HTTPS beacons for short haul because the amount of data they collect on target systems. Beacons are better than long, persistent connections like Metasploit payloads do. An excellent article about detecting long connections is available from our friends at Black Hills Information Security. In the APT19 Threat Thursday we covered how to identify beacons over HTTPS. This week, lets focus on detecting DNS C2. Our friends at Active Countermeasures have use covered.

Conclusion

In this week's #ThreatThursday we learned how to consume cyber threat intelligence, extract TTPs, and build an adversary emulation plan when the MITRE ATT&CK website does not have the group documented. We also learned that Buhtrap uses short haul and long haul C2 over HTTPS and DNS respectively. This is common among sophisticated threat actors and important to have detective controls around. Hope you enjoyed!

About SCYTHE

SCYTHE provides an advanced attack emulation platform for the enterprise and cybersecurity consulting market. The SCYTHE platform enables Red, Blue, and Purple teams to build and emulate real-world adversarial campaigns in a matter of minutes. Customers are in turn enabled to validate the risk posture and exposure of their business and employees and the performance of enterprise security teams and existing security solutions. Based in Arlington, VA, the company is privately held and is funded by Gula Tech Adventures, Paladin Capital, Evolution Equity, and private industry investors. For more information email info@scythe.io, visit https://scythe.io, or follow on Twitter @scythe_io.