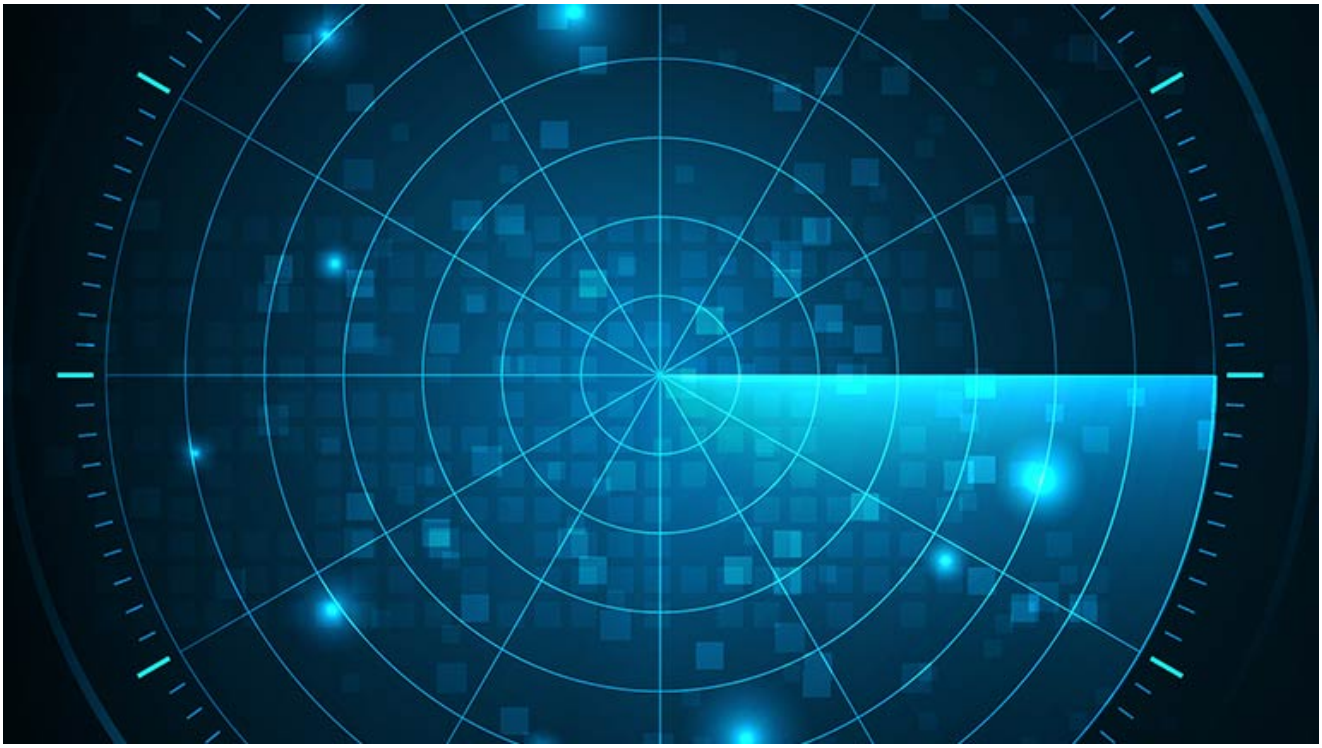
Turla uses HyperStack, Carbon, and Kazuar to compromise government entity

accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity



Turla, identified internally by Accenture Cyber Threat Intelligence as Belugasturgeon, continues to target government organizations using custom malware, including updated legacy tools, designed to maintain persistence through overlapping backdoor access while evading their victim's defenses. One such tool, the HyperStack backdoor (named after its filename on one identified sample), has seen significant updates that appear to be inspired by the group's Carbon backdoor and the RPC backdoor described by ESET researchers.

Turla has conducted espionage operations on behalf of its state sponsor for over a decade. The group primarily targets foreign governments and embassies using advanced custom tools designed to stay hidden for long periods of time. The activity identified by Accenture threat researchers is within the group's typical targeting set using their custom tools, albeit with some updates.

Tactics

Accenture Cyber Threat Intelligence researchers identified a Turla compromise of a European government organization. During this compromise Turla utilized a combination of remote procedure call (RPC)-based backdoors, such as HyperStack and remote administration trojans (RATs), such as Kazuar and Carbon, which ACTI researchers analyzed between June and October 2020. The RATs transmit the command execution

results and exfiltrate data from the victim's network while the RPC-based backdoors use the RPC protocol to perform lateral movement and issue and receive commands on other machines in the local network. These tools often include several layers of obfuscation and defense evasion techniques.

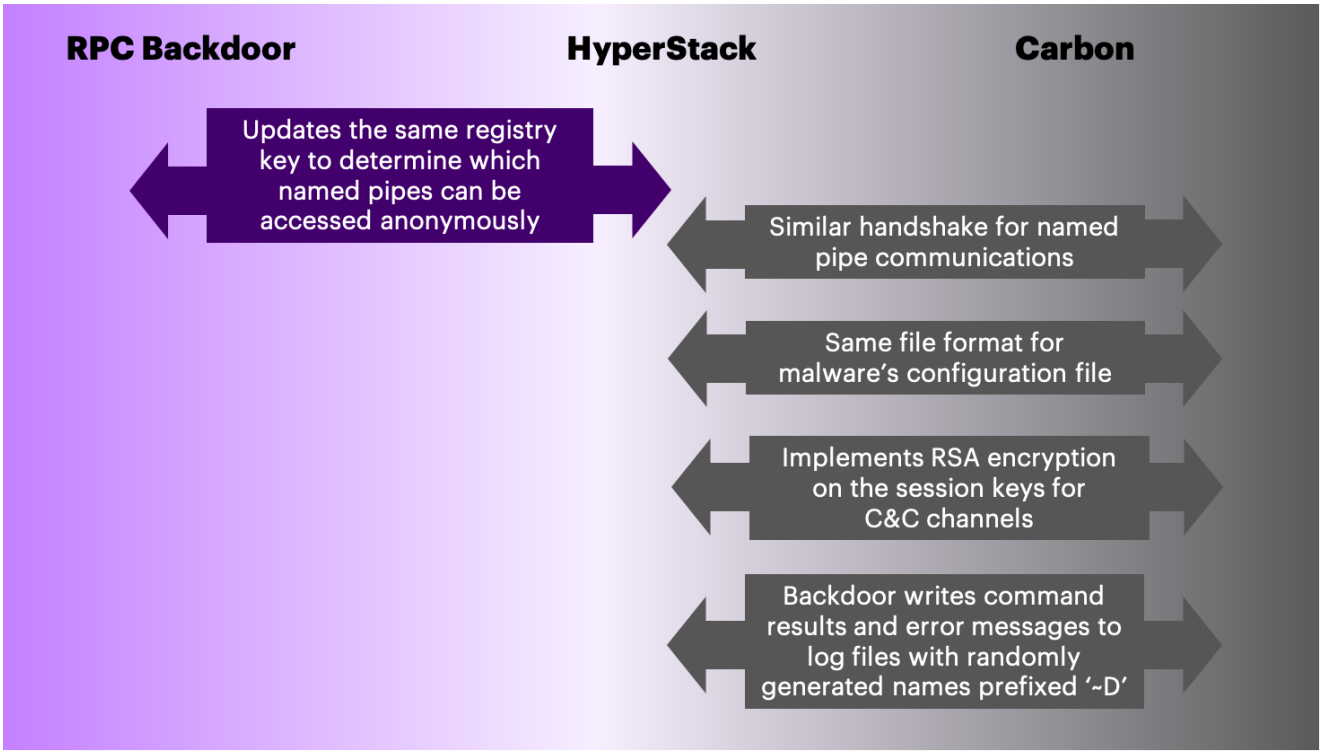
This combination of tools has served Turla well, as some of their current backdoors use code that dates back to 2005, according to Palo Alto researchers. The threat group will likely continue to maintain and rely on this ecosystem, and iterations of it, as long as the group targets Windows-based networks.

Turla uses a variety of command and control (C&C) implementations within each compromise which allows for multiple avenues of reentry if parts of the compromise are identified by defenders. Notably, Accenture researchers recently identified novel command and control (C&C) configurations for Turla's Carbon and Kazuar backdoors on the same victim network. The Kazuar instances varied in configuration between using external C&C nodes off the victim network and internal nodes on the affected network, and the Carbon instance had been updated to include a Pastebin project to receive encrypted tasks alongside its traditional HTTP C&C infrastructure.

HyperStack functionality

HyperStack, first observed in 2018, is one of several RPC backdoors Turla uses. A sample identified in September 2020 has updated functionality which appears to be inspired the RPC backdoors previously publicly disclosed by ESET and Symantec Researchers as well as with the Carbon backdoor. Based on these similarities, we assess with high confidence that HyperStack is a custom Turla backdoor.

<<< Start >>>

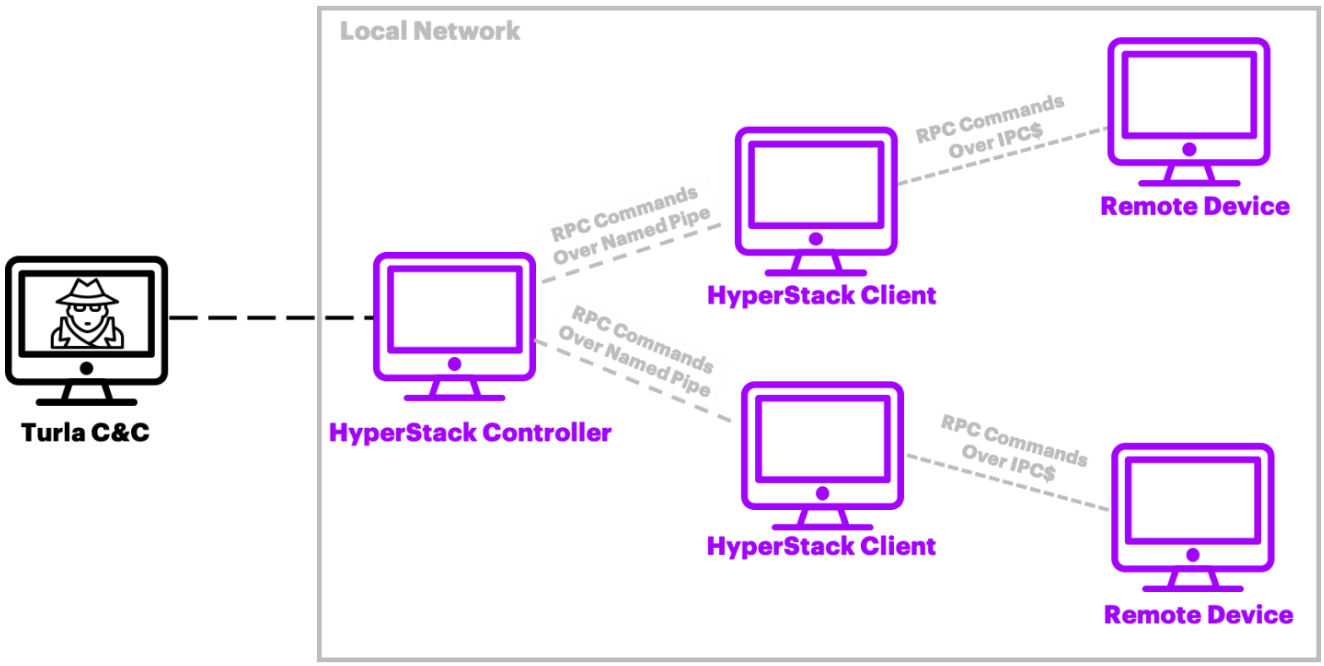


Comparison of Hyperstack to Turla's carbon and RPC backdoors

<<< End >>>

HyperStack uses named pipes to execute remote procedure calls (RPC) from the controller to the device hosting the HyperStack client. To move laterally, the implant tries to connect to another remote device's IPC$ share, either using a null session or default credentials. IPC$ is a share that facilitates inter-process communication (IPC) by exposing named pipes to write to or read from. If the implant's connection to the IPC$ is successful, the implant can forward RPC commands from the controller to the remote device, and likely has the capability to copy itself onto the remote device.

<<< Start >>>



HyperStack usage

<<< End >>>

Another version of HyperStack observed in this campaign contained a simpler functionality, allowing Turla operators to run commands via a named pipe from the controller to the implant, without any of the IPC$ enumeration activity.

Varied command and control

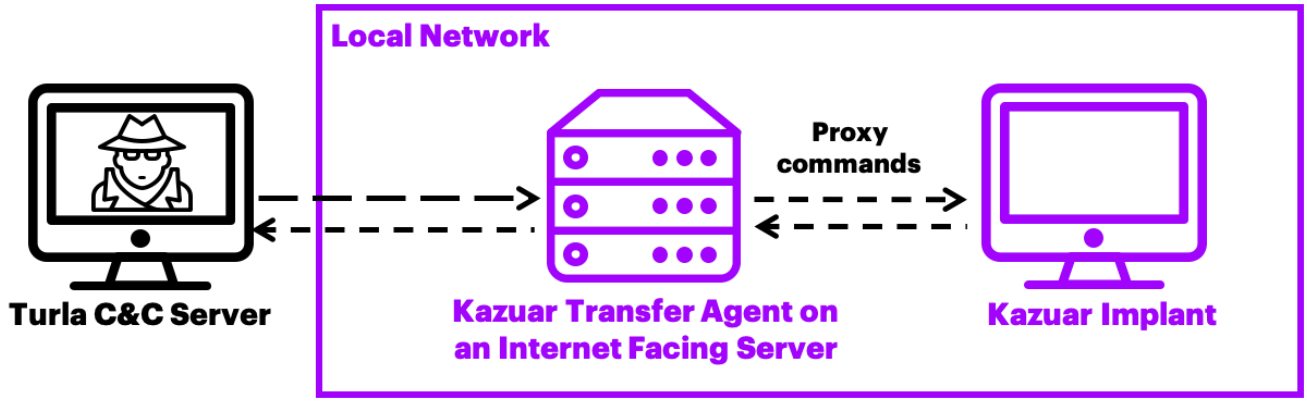
Analysis of several backdoors identified in this recent operation revealed that Turla has relied on traditional C&C implementations, using compromised web servers as C&C, as well as utilizing legitimate web services like Pastebin. Additionally, one analyzed sample of Kazuar is configured for commands sent through likely internal nodes in the government's network, while others use the more traditional method of external C&C nodes. Varying the C&C ensures multiple avenues of recovery into the network if some of the group's accesses are found and remediated against by network defenders.

Kazuar - Command and Control

In mid-September, we analyzed a sample of Kazuar that, unlike traditional Kazuar samples, is configured to receive commands via Uniform Resource Identifiers (URI) pointing to internal C&C nodes in the victim government network.

This Kazuar configuration acts in conjunction with another sample, analyzed in early October, on the same victim network. Based on references to the internal C&C node, the October sample likely acts as a transfer agent used to proxy commands from the remote Turla operators to the Kazuar instances on internal nodes in the network via an internet-facing shared network location. This set-up allows Turla operators to communicate with Kazuar-infected machines in the victim network that are not accessible remotely.

<<< Start >>>

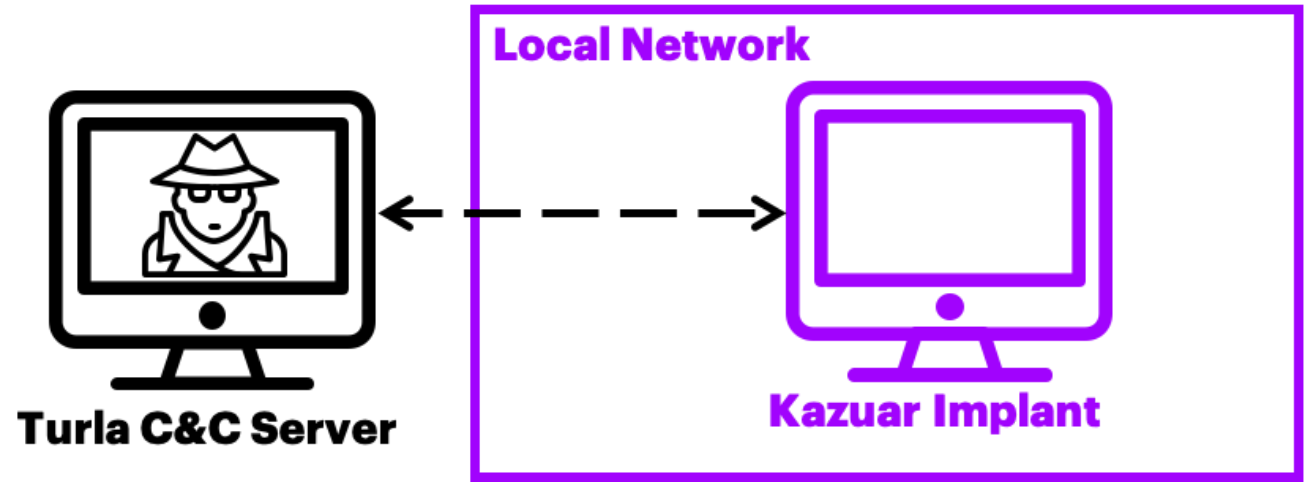


Kazuar C&C unique implementation

<<< End >>>

Another recently analyzed sample of Kazuar from the same victim network had a traditional C&C implementation where the implant communicates directly with a C&C server located outside the victim network. The C&C URLs correspond to compromised legitimate websites for Turla to proxy commands and exfiltrate data to Turla backend infrastructure.

<<< Start >>>



Kazuar C&C traditional implementation

<<< End >>>

Carbon - Command and control using Pastebin

Turla has extensively used Carbon, a modular backdoor framework with advanced peer-to-peer capability, for several years. A June 2020 analyzed instance of the Carbon backdoor augmented the traditional threat actor-owned C&C infrastructure with tasks served from Pastebin, a legitimate web service. The Carbon installer discovered by ACTI analysts dropped a Carbon Orchestrator, two communication modules, and an encrypted configuration file.

The configuration file contains C&C URLs traditionally observed in Carbon instances, which are likely compromised web servers hosting a web shell that transmits commands and exfiltrates data from the victim network. It also contains a parameter labeled [RENDEZVOUS_POINT] which contains a URL for a Pastebin project.

When accessing the Pastebin URL, an encrypted blob is downloaded that requires a corresponding RSA private key from the configuration file. The configuration file analyzed did not contain the RSA private key and therefore we were unable to decrypt the contents of the Pastebin link. We assess the decrypted blob was likely a task for the Carbon instance.

Exploiting legitimate web services for C&C

We are increasingly observing cyber-espionage groups use legitimate web services for their operational command and control, and Turla is no exception to this trend.

Groups likely use these services for several reasons:

- Web services allow cyber-espionage groups' malicious network traffic to blend easily with legitimate network traffic
- Threat groups can easily change or create new infrastructure which makes it difficult for defenders to shut down or sinkhole their infrastructure
- Using web services complicates attribution since the C&C infrastructure is not owned by the threat group

Additionally, web services have the added benefit of being free or inexpensive and requiring limited resources for creation and maintenance.

Conclusion

Turla will likely continue to use its legacy tools, albeit with upgrades, to compromise and maintain long term access to its victims because these tools have proven successful against windows-based networks. Government entities, in particular, should check network logs for indicators of compromise and build detections aimed at thwarting this threat actor.

The Accenture Cyber Threat Intelligence (ACTI) team provides actionable and relevant threat intelligence to support decision makers. The intelligence analysis and assessments in this report are grounded in verified facts; more information on this activity is available to subscription customers on ACTI IntelGraph. IntelGraph is a proprietary next generation security intelligence platform that allows users to search, visualize, and contextualize the relationships between malicious actors, their tools and the vulnerabilities they exploit.

MITRE ATT&CK techniques

Tactic	Technique ID	Technique name

Execution	T1059 T1569	Command-line Interface Service Execution
Persistence	T1543	New Service
Privilege Escalation	T1543	New Service
Discovery	T1135 T1012	Network Share Discovery Query Registry
Lateral Movement	T1021	Windows Admin Shares
Command and Control	T1102 T1001 T1090 T1071	Web Service Data Obfuscation Proxy Standard Application Layer Protocol

Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Technical details

HyperStack Execution Routine

Upon execution, HyperStack undergoes a similar registry key check to Turla's RPC backdoor and updates the same registry key to determine which named pipes can be accessed anonymously. The HyperStack backdoor first copies itself to C:\ADSchemeIntegrity.exe and then installs itself with system-level privileges as the service Active Directory Scheme Integrity Service. HyperStack checks for the following registry entry and, when found, adds the name of its communication pipe ('adschemerpc') to the key value:

HKLM\SYSTEM\\CurrentControlSet\\Services\\lanmanserver\\parameters\NullSessionPipes

To make the pipe available to anyone, HyperStack sets the security descriptor for the pipe to S:(ML;;NW;;;S-1-16-0)—a method that Turla also uses in its RPC backdoor.

HyperStack Custom Handshake

Next, HyperStack uses a custom handshake that is similar to handshakes used for Carbon named-pipe communications. To detect incoming connections from the controller, the HyperStack implant uses the Windows API call 'ConnectNamedPipe'. When HyperStack receives an incoming connection, it starts a new thread and continues with the custom handshake. The malware reads 8 bytes from the pipe and checks if it matches : B19B055CA11CACA0. If it matches, the HyperStack implant returns the value CACA05ACCE55F11E to the controller. Similar 8-byte hex values are exchanged as part of the Carbon backdoor's custom handshake.

Configuration file

HyperStack writes a configuration file named backport.inf, the same file format as the Carbon malware's configuration file. The configuration file is written to %SystemRoot%\INF\backport.inf and contains a [Version] section with various keys:

<<< Start >>>

```
[Version]
Type=SilentMoon
CLSID=kNAiAOAj2KAhaJan
```

Figure 1. HyperStack configuration file

<<< End >>>

The [Version] section of the file contains several keys that the malware writes including:

- Type – Likely a form of version control. The malware sets the Type key to SilentMoon.
- CLSID – The class ID for the implant seeded with a call to rand().
- PRVK – Stores the RSA key pair needed for session key encryption.
- Revision and Signature – Read from the file prior to RSA key generation.

HyperStack checks the configuration file to determine if the Type equals SilentMoon. If yes, it generates an RSA PKCS key using CryptGenKey that is used for encryption of communication session keys. It then writes the RSA key to the PRVK key in the [Version] section of the config file. Turla's Carbon backdoor also implements RSA encryption on the session keys for some of its C&C channels.

Use of inter-process communication (IPC$) share

HyperStack sets the registry key HKLM\SYSTEM\CurrentControlSet\Control\LSA\Restrict Anonymous value to 0 so anonymous logon users (i.e., null session connections) can list all account names and enumerate all shared resources on a remote share. The implant can then use the WNetAddConnection2 API call to connect to another remote device's IPC$ share. IPC$ is a share that facilitates inter-process communication (IPC) by exposing named pipes to write to or read from. The implant attempts to connect to the IPC$ share using a null session, or if this fails, with default credentials.

HyperStack uses named pipes to execute remote procedure calls (RPC) from the controller to the device hosting the HyperStack implant. If the implant's connection to the IPC$ is successful, the implant can forward RPC commands from the controller to the remote device, and likely has the capability to copy itself onto the remote device.

Turla also used the IPC$ share during the lateral movement stage of its compromise of Swiss defense firm RUAG, according to the Swiss Government Computer Emergency Response Team's technical report describing the incident.

Message and log files

The HyperStack implant writes command results and error messages to log files stored in the %Temp% directory. The log files have randomly generated names with the prefixes 'sm' and '~D'. Turla uses the same '~D' prefix for the names of Carbon log files. The HyperStack implant also searches for log files with the prefix ~X and deletes them, suggesting it may be cleaning up after previous versions or another malware family's logs.

Another version of HyperStack observed in this campaign contained a simpler functionality, allowing Turla operators to run commands via a named pipe from the controller to the implant, without any of the IPC$ enumeration activity.

The similarities between the updated functionality in the HyperStack implementation found in September 2020, the RPC backdoor, and the Carbon malware suggest these HyperStack updates were inspired by Turla's other malware operations, potentially in response to remediation activity taken by the victim.

IOCs

To mitigate the threat of Carbon, Kazuar, and HyperStack, ACTI recommends checking network logs for indicators related to these backdoors including the following IOCs:

SHA256	Filename	NAME
e888b93f4d5f28699b29271a95ccad55ca937977d42228637ad9a7c037d3a6a4	DebugView.exe	Kazuar backdoor
1f7b35e90b5ddf6bfd110181b1b70487011ab29ca5f942170af7e8393a1da763	Agent.exe	Kazuar backdoor
1fca5f41211c800830c5f5c3e355d31a05e4c702401a61f11e25387e25eeb7fa	RuntimeBroker.exe	Kazuar backdoor
60000bc2598eff85a6a83d5302fc3ed2565005d8fd0d9f09d837123a1599ef8d	WSUSTransfer.exe	Kazuar Backdoor
493e5fae191950b901764868b065ddddffa4f4c9b497022ee2f998b4a94f0fc2	DSCEBIN.EXE	Carbon Installer
f3aaa091fdbc8772fb7bd3a81665f4d33c3b62bf98caad6fee4424654ba26429	sacril.dll	Carbon Orchestrat
2b969111dd1968d47b02d6390c92fb622cd03570b02ecf9215031ff03611a2b7	ablhelper.dll	Carbon Communic File
7d5794ad91351c7c5d7fbad8e83e3b71a09baac65fb09ca75d8d18339d24a46f	frontapp.dll	Carbon Communic File
8ef22c8b5d6bc2445d3227650804b2e1435a5f986134a9aa7e07f3b948921b5b	estdlawf.fes	Carbon Configurat File
6ca0b4efe077fe05b2ae871bf50133c706c7090a54d2c3536a6c86ff454caa9a	ADSchemeIntegrity.exe	HyperStac
722fa0c893b39fef787b7bc277c979d29adc1525d77dd952f0cc61cd4d0597cc	101_iex_memory_code_exe.exe	RPC back

97187123b80b1618f0d8afc2a5f84e9a17ac8e53a6e4ce8b0aa39fe06cec1f36	1.ps1	Reflective PowerShe loader
20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5	hyperstack.exe	HyperStac
e33580ae3df9d27d7cfb7b8f518a2704e55c92dd74cbbab8ef58ddfd36524cc8	ADSchemeIntegrity.exe	HyperStac

C&C URLs for Carbon implant

www.berlinguas[.]com/wp-content/languages/index.php
www.balletmaniacs[.]com/wp-includes/fonts/icons/
pastebin[.]com:443/raw/5qXBPmAZ
suplexrpc – Named pipe

C&C URLs for Kazuar implant

https://www.bombheros[.]com/wp-content/languages/index[.]php
https://www.simplifiedhomesales[.]com/wp-includes/images/index.php
http://mtsoft.hol[.]es/wp-content/gallery/
http://www.polishpod101[.]com/forum/language/en/sign/