Die rasante Evolution von Latrodectus geht mit den neuesten neuen Nutzlastfunktionen weiter

By Leandro Fróes

Published: 2024-08-29 · Archived: 2026-04-05 14:28:39 UTC

Zusammenfassung

Latrodectus ist ein Downloader, der erstmals im Oktober 2023 von Walmart entdeckt wurde. Die Malware wurde aufgrund ihrer Ähnlichkeiten mit der berühmten IcedID-Malware sehr berühmt, nicht nur im Code selbst, sondern auch in der Infrastruktur, wie zuvor von Proofpoint und Team Cymru S2 berichtet wurde .

Die Malware wird in der Regel über E-Mail-Spam-Kampagnen verbreitet, die von zwei bestimmten Bedrohungsakteuren durchgeführt werden: TA577 und TA578. Zu den verschiedenen Funktionen, die es enthält, gehört die Möglichkeit, zusätzliche Nutzlasten herunterzuladen und auszuführen, Systeminformationen zu sammeln und an den C2 zu senden, Prozesse zu beenden und vieles mehr. Im Juli 2024 wurde auch Latrodectus beobachtet , wie er von einem BRC4-Dachs entbunden wurde.

Während der Jagdaktivitäten in den Threat Labs haben wir eine neue Version der Latrodectus-Payload entdeckt, Version 1.4. Die Malware-Updates umfassen einen anderen Ansatz zur Entschleierung von Zeichenfolgen, einen neuen C2-Endpunkt, zwei neue Backdoor-Befehle und vieles mehr.

In diesem Blog konzentrieren wir uns auf die Funktionen, die in dieser neuen Version hinzugefügt/aktualisiert wurden.

Analyse von JavaScript-Dateien

Die erste Nutzlast der Infektionskette ist eine JavaScript-Datei, die mit einem ähnlichen Ansatz verschleiert wurde, der von anderen Latrodectus-Kampagnen verwendet wird. Die Verschleierungstechnik wird verwendet, indem der Datei mehrere Kommentare hinzugefügt werden, was die Analyse erschwert und die Dateigröße erheblich erhöht.

Der relevante Code befindet sich zwischen den Junk-Kommentaren und sobald er aus der Datei entfernt wurde, können wir den Code sehen, der ausgeführt werden würde.

Die Malware sucht nach Zeilen, die mit dem String "/////" beginnen, legt sie in einen Puffer und führt sie als JS-Funktion aus. Die ausgeführte Funktion lädt dann eine MSI-Datei von einem Remote-Server herunter und führt sie aus/installiert sie.

Analyse von MSI-Dateien

Nach der Ausführung/Installation verwendet die MSI-Datei das rundll32.exe Windows-Tool, um eine DLL mit dem Namen "nvidia.dll" zu laden und ruft eine Funktion mit dem Namen "AnselEnableCheck" auf, die von dieser DLL exportiert wird. Die bösartige DLL wird in einer CAB-Datei mit dem Namen "disk1" gespeichert, die in der MSI-Datei selbst vorhanden ist:

Kryptor-Analyse

Als Versuch, die Hauptnutzlast zu verschleiern, die "nvidia.dll" file verwendet einen Crypter namens Dave. Diesen Crypter gibt es schon seit langer Zeit und wurde in der Vergangenheit von anderer Malware wie Emotet, BlackBasta und früheren Versionen von Latrodectus verwendet.

Der Crypter speichert die Payload, die ausgeführt werden soll, entweder in einer Ressource oder in einem Abschnitt. In der analysierten Probe wird die Nutzlast in einem Abschnitt mit dem Namen "V+N" gespeichert.

Die Schritte zum Entschleiern, Laden und Ausführen der endgültigen Nutzlast sind recht einfach. Die Malware verschiebt einen Schlüssel in den Stack und löst die Windows-API-Funktionen VirtualAlloc, LoadLibrary und GetProcAddress auf.

Anschließend wird der Speicher mithilfe der VirtualAlloc-Funktion zugewiesen und eine Multi-Byte-XOR-Operation für die Daten im genannten Abschnitt unter Verwendung des zuvor festgelegten Schlüssels ausgeführt, und das Ergebnis der Operation ist die endgültige Nutzlast. Die nächsten Schritte umfassen das Ausrichten der Nutzlast im Speicher und den Aufruf ihrer Hauptfunktion.

Da der Crypter zuerst die ursprüngliche Nutzlast in den zugewiesenen Speicher kopiert, bevor die anderen Schritte ausgeführt werden, kann man einfach den Inhalt des ersten zugewiesenen Speichers ausgeben und die endgültige Nutzlast abrufen. Ein Skript zum statischen Entpacken/Entschleiern von Latrodectus-Payloads mit dem Dave-Crypter finden Sie hier.

Die endgültige Nutzlast ist eine DLL, und ihre DllMain-Funktion wird vom Verschlüsselungscode aufgerufen. Der nächste Schritt ist die Ausführung der exportierten Funktion "AnselEnableCheck", die für die Ausführung der finalen Payload verantwortlich ist.

Wenn wir uns die endgültige Nutzlast ansehen, stellen wir fest, dass sie mehrere exportierte Funktionen hat, obwohl es keine Rolle spielt, welche aufgerufen wird, da alle die gleiche RVA haben.

Latrodectus-DLL-Analyse

Da die allgemeinen Merkmale der Hauptnutzlast bereits in der Vergangenheit von anderen Forschern beschrieben wurden, konzentrieren sich die folgenden Abschnitte auf die Updates, die von der neuen Latrodectus-Version verwendet werden.

Zeichenfolgenverschleierung

Im Gegensatz zu den vorherigen Versionen, die eine XOR-Operation zum Entschleiern der Zeichenfolgen verwendeten, verwendet die aktualisierte Version AES256 im CTR-Modus. Der AES-Schlüssel ist in der Entschleierungsfunktion selbst fest codiert, und der IV ändert sich für jede Zeichenfolge, die entschlüsselt werden soll. Der Schlüssel, der in den analysierten Proben verwendet wird, lautet "d623b8ef6226cec3e24c55127de873e7839c776bb1a93b57b25fdbea0db68ea2".

Die Entschleierungsfunktion erhält zwei Parameter. Der erste ist ein Datenblock und der zweite ein Ausgabepuffer. Der Datenblock wird zum Speichern von Informationen verwendet, die zum Entschlüsseln der Zeichenfolge verwendet werden, und hat das folgende Format:

- Länge der Zeichenfolge: 2 Bytes
- IV: 16 Byte
- Verschlüsselte Zeichenfolge: Im ersten Feld angegebene Größe

Zu beachten ist, dass nach dem verschlüsselten Zeichenfolgeninhalt manchmal zusätzliche Bytes stehen. Die folgende Abbildung ist ein Beispiel für diesen Datenblock:

Kampagnen-ID

In der aktuellen Malware-Version verwendet die Funktion zur Generierung von Kampagnen-IDs weiterhin den gleichen Ansatz, bei dem eine Eingabezeichenfolge mit dem FNV-Algorithmus gehasht wird. Es wurde jedoch ein neuer Eingabestring "Wiski" verwendet, was dazu führte, dass der Hash als Kampagnen-ID 0x24e7ce9e.

C2-Kommunikation

Für die erste Kommunikation mit dem C2-Server sammelt Latrodectus viele Informationen vom infizierten System wie den Benutzernamen, die Betriebssystemversion und die MAC-Adresse. Die Informationen werden nach einem bestimmten Muster formatiert, mit dem RC4-Algorithmus verschlüsselt, mit base64 codiert und an den C2 gesendet.

Die RC4-Schlüssel, die in den analysierten Proben gefunden wurden, waren "2sDbsEUXvhgLOO4Irt8AF6el3jJ0M1MowXyao00Nn6ZUjtjXwb" und "kcyBA7IbADOhw5ztcv09vmF8GYmR38eu7OGdfD7pyRelTPKH1G".

Bei der Datenformatierung können wir die Versionsnummer 1.4 markieren, die gesetzt wird.

Die Informationen werden im HTTP-Body über eine HTTP POST-Anfrage gesendet. Der Endpunkt, der in den neuen Varianten verwendet wird, ist "/test" anstelle von "/live", wie in früheren Versionen beobachtet. Obwohl dies ein sehr schwacher Indikator ist, könnte die Verwendung dieses speziellen Endpunkts darauf hindeuten, dass es sich um eine Testversion der Malware handelt.

Befehle

In Version 1.4 hat Latrodectus zwei neue Befehle in seine Payload eingeführt: Befehls-ID 22 und 25.

Befehl 0x16

Bei diesem Befehl lädt die Malware einen Shellcode vom angegebenen Server herunter und führt ihn über einen neuen Thread aus.

Der Unterschied zwischen diesem Befehl und Befehl 14 besteht darin, dass eine Funktion, die die Base64-Codierung ausführt, als Parameter an den Shellcode selbst übergeben wird. Die Adresse der base64-Funktion wird in einer zugeordneten Dateiansicht mit dem Namen "12345" gespeichert.

Befehl 0x19

In diesem Befehl erhält die Malware einen Dateinamen und einen Remote-Speicherort, von dem die Datei heruntergeladen werden soll. Der Dateiname wird dann an %AppData% angehängt, die Datei wird heruntergeladen und ihr Inhalt in den angegebenen Pfad geschrieben.

Unter Berücksichtigung dieser Ergänzungen finden Sie im Folgenden eine Tabelle der aktualisierten Befehle, die von der Malware unterstützt werden:

Befehls-ID	**Description**
2	Sammeln einer Liste von Desktop-Dateinamen
3	Sammeln von Informationen über die laufenden Prozesse
4	Sammeln von Systeminformationen
12	Laden Sie eine reguläre ausführbare Datei herunter und führen Sie sie aus
13	Herunterladen und Ausführen einer DLL über rundll32
14	Laden Sie einen Shellcode herunter und führen Sie ihn aus
15	Selbstaktualisierung

Befehls-ID	Description
17	Beenden Sie sich selbst
18	Laden Sie die IcedID-Nutzlast herunter und führen Sie sie aus
19	Erhöhen Sie die Zeitüberschreitung im Ruhezustand
20	Anforderungszähler zurücksetzen
21	Laden Sie das Stealer-Modul herunter und führen Sie es aus
22	Laden Sie einen Shellcode herunter und führen Sie ihn aus, indem Sie die base64-Codierungsfunktion als Parameter übergeben
25	Laden Sie eine Datei in das Verzeichnis %AppData% herunter

Netskope-Erkennung

- Netskope Threat Protection
  - Gen:Variant.Ulise.493872
  - Trojaner.Generic.36724146
- Netskope Advanced Threat Protection bietet proaktiven Schutz gegen diese Bedrohung.
  - Win64.Trojan.ShellCoExec

Schlussfolgerungen

Latrodectus hat sich ziemlich schnell weiterentwickelt und seiner Nutzlast neue Funktionen hinzugefügt. Das Verständnis der Aktualisierungen, die auf die Nutzlast angewendet werden, ermöglicht es Defendern, automatisierte Pipelines ordnungsgemäß einzurichten und die Informationen für die weitere Suche nach neuen Varianten zu verwenden. Netskope Threat Labs wird weiterhin verfolgen, wie sich der Latrodectus entwickelt und wie viel TTP er hat.

IOCs

Alle IOCs und Skripte, die sich auf diese Malware beziehen, finden Sie in unserem GitHub-Repository.
