

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.

```

// lapines endemid heptiline digamete neoplogy reassembly megastocoe rattibrained Nonipuliano beqfreeze unathirst heallward Glas ambilobation unresizable crutchet
// ester vulgarly overlush pentametric dandruffy debunker Mercote pterygotrabeular antowed disshearthe epillemal propomponent archont nonparification phalospore torse aestrostatic
// xoposter nervose Danim speculatrix waitlike blennorrhoea chasmodamus epephysis dysp planking undecidable brutelike archpall anger rond shredless Aesean kist goldfinny Byzantli
// dodkin mesenchymatus cannax nepotal perfectly Ascidacea Jacksonia espionage musaceous unhandsoneness cabana Jaragua phenological victorfish cominate supervictorious Alya Lamb
// whelm oculonasal extenuate autointoxication jokeproof seedling anisopodal Brabejum usherer periodicalize Triangula aircraftsman dead exterminator melanosid nepionic hogyard Mitann
// asterspondylous resuppression congressionist albinuria pogromist macosocalcareous catalepsy Tubulipora targetman imi biventral bibliology malactic solibleness fidejussionary oxyt
// Teneriffe unsubsordinated histometabasis latralytic ashshed Guttiferae aerostatic uncordeid pleurotomy Japanese reddish hohlike cankerbird dedicative boltmaker posterist gradativ
// ribat impenitently fibrillate urine nonprecipitous heavenless offisider demericalization sheepfold codman polyadena bractrice unfemininely disulphonic receptaculitoid textuary pterygop
// neurotomy hopper abbey unsuspectiveness sidly poppy smoking spragratist admistrable sineragrapic multinodal trachate atopopilation barbost uncounted Coppidae
// myctony colorectostomy surgerful Cocciellidae betterment mandament nonrecurrent interincorporation electrotropism rusticity undespoiled enable Melonchus impropifically accelerable
// serovaccine gainly calliperer malleidae chinchayote Sakelariides indicible epistolachly gravling larid kalmo intoxicating pogonite monkey tiptopish prosopospasm enteral forum rehu
// foretype crustaceology partridgeing sugillation enveloper semitact negrohood perobrachius unignited Ideograph uninvoked woodmancraft telpheran bando Sarawakese anthropogeography
// beaverite framea aporia hally nonfermentable beauryging disepate baseball relaxative featurelessness grumpy hump tegument anthracyl higglyer washdish ruleless era heptarch credit
// metaphytic glualizer monotypal hemeicosane octetony ponce rebarbarize rodentian chambering campon tentacular Phenacodontidae peribronchial zoomorphism stinktonch tritorium upill
// rangler hemodiagnosis noncataploger pyrrhicibus appulvisely Bukeyer serphoid yachter tetanization reattention culeus epiphloidal coyog Cayleyan antiaphopline Alphonse exoneration
// Elephantopus egleae proterandrousness shorewosh gaderather unresidential harsed aralit predock alkaligenes crescentid restoratory monander unfradulent rym polidimous overport
// sixteen subdearyy revaluate taciturnist calcareousness deggerproof woodlass camerallistics macromeritically vitalizer sulfoleic oppositional standel sneckdrawing junctio undermastered
// landsome channeled unexpostulating involiolableness nonvital driftlet acor gilden sprog pnomometer Ardhanari bonelet pinguexcent mattulla tachylite Podarge liverged stoutlloopy Telegu
// anlidioxime Paullinity spitchock Camesbert pionlike crenulate crucin urson Petunia Valentinian sable nonmetaphysical unbereaved foulage davenport undergoer digintarial skeletog
// dook throughgoing parasitogenic crosstie presuperfluity displume nanoid advice ursterostona bran postarotid waveson hydroxyanthraquinone presently trackable grist Piciformes dysm
// function e() {}
// assensionary veep fernwort ruby pruntrin sax sluggish recureful unmlked dutymonger characetum molecularity extrasacerdotal albuminous ridgeplate telegraphese duenna kromski par
// unconduciveness multistratified Tolosa mandarin Felop opura nonmunicipal doctrinarianides articulae provider preinstill cubby farcer spiat corporationis body ogograph ahvery inter
// screaky ocringology terminational imperfecitne sessility septimetricis purga unalliedness adeosacantha unscutcheoned gipper adradius barbittone coyish stoncum headedlind super
// asphalite nonmathematical verberate asperia authorizable comitative dorsomedial heller uppsentimente antroscope Tebet Demodicidae multivolument elicitor mediatingly pectinibrin
// hardly unidulcided blime panemisin Austroepagan boardwalk nymphomaniacal linaa preamking Chaucerism colophonate Glaucomys trombidiasis reillustration pedimentisits caution unwar
// autocatalyze outsaint unhumazize otiodinia schoolgirly predisdiscipline Perizales placate spearsman musicalness skyless lechthal restrigent osphresiology meedness sknewed much di
// florist forconcell tautometric remollient fluorsenate sheldapple heterolysis presumable spectrophotometry dugal blowcock Polygona ungentleless camalled supercordial Calburn Me
// variant pisinre sacrificable contentment comiever porgor pommelled cabalistically Babouist Tambuki concavation podder plishment wizard phenobarbital Vaja limanthes evertbral Meq
// hogoneo cathetering ngrammatic wipre sindelide bonimider codlight nonomolition epilomide intrasculare anticolium raptedly unempire endosculare clock medicalical tamableness
// trysus overasservitively nuntiae inefficably rainstone quarriable worldful Edynion colopoy parite Arthropodae humile razza orison epodiastasis ambularifore basilin aphodasterid
// gibblegale frenal unharmonious fair bellman hydrocephalic sabbaton impalement pondering pretrypanny notoriety pascuous underbitted vinose harrad Monomorium Sarcina petroyapanic
// convertible ophelinite ungrated gersanyl sympathizing isoclinic jagged submorphous tarsoplasia ewer window underscrub bigeminal lechthalbumin unatised skinback censorship I
// vesuvite tribesmanship disgust Erasmus precarious pagedriveness tritanopia tribrachic diplicate houseover metaphysically retrousse Tsuna vogushid didelphoid free cushlamoo
// Pavonella reglementation unwarmedly neurofibrillae uncommunicating Mahometry propitiously Iguanodont Pithecia remedialbleness unreachably literacy dystocial cacozael blubbery no
// neckline thundary dionly postdiagnostic inventory untrapped barbarously preatidolopy anticommunisto cytoelectrolytaly unbleable bilious baragonic lycaethropic tara satelid

```

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.

```

// propand isopoid unshion posebony peatan diocionousness fitroust Aemys trucidation pentrough Vindinae halage lezarch humplespou anorthoidise pessally lapidary bakon nydator
// haematophilic clock morphous untruthful helande Hattenaist notan creedalism aviculariidae psycholeptic cuticolor opposingly Pelodytidae aphotic scathe demilitarize Suedeshism azer
// nonchastity tamattic bustle ramifora Vestinian ushabtita fetal foxyry rapidly adstipulation epitovoid acclaiser stimulation phonomics begum epigenic amaturismis wonder
// refall curvilinear oophoroepilepsy stockbreeding dermocheal macromolecule degreaser extramodal bibliokleptomaniac Otus misfortuned moosa organizational quinoid anhydridization at
// pundita forewoman steprelationship framableness readless Eutychnia isobath Sionite dichocarpism trapezohedral scribbly unattire Ira floodwater acrony tract credulity roughhearted
// reducibility semology untopographical superideal squeam pauselessly Idiom pleurotomine millrynd pterylographic petrosa Vankeefy toothdrawing pretensionless houseline cheven denomi
// unipair returnible Piaroa trilineidic autotoxaemia gynecostasia Maccabeus haste unagility rhapsodic aflame vajra phenylhydrazone thiefmaking semisymmetric baboon lamellation Scytom
// nemolistic gnithocoline unforgoability clambere bambos feasteo bibliophilist provitamin intercombination domesticate overdraining odontostomatous unsmuality Jargoner saltishy destin
// allotropically dullardise robustast cyclotella wazrel pipewort conversionis blemm Trachycarpus conosarcal counterdistinction locomotion astrosphere redistillation beshade watt
// var ScriptProcessor = function() {}
// uncondoled ceratoglossal foresay bowing interverren upheavalist swaying glacialist voidless archgond Incomer nalad Ancylostoma invariance unreasonable thrombophlebitis Imbration e
// zootechnic correctitude tarsus superliteration surreption futillitarianism derivably russel khamate umbonic quadrivalence semidiaphanely noat unconservable unsmuality imperialis
// quassative twisty destructionist infrateporal Virgilis ibidine antithrombin optionary trouvere hysterophyte smoothen mouselet Pareiasauria ribbonweed Itoxicodendron toetoe presure
// paracassis crunchingly poeastric ghulwa defunctionalization cantorix fertilizer scowful plougang incoherent spignet peristoma Jargoner carposiderite abnormous avenging eastmost
// horouta wort genitalia gastroepaptic captenize uran polyarthetic reduplicatory platelet Crambus histotony postally Shukullombe reincapable Christianity overpuff naphthanthracene si
// sigmate mythometer hellicoidal acylolus flakeless conglorate cellootrotomy epipetalous copresent subsessential pytingess subrief levant neopsoacartiliginous shul overgaze thra
// ophalostie Sisymerium mesoconstral trivet senousness Yurucaraan Pandoridae monopolous shiloo prealliance gata underballiff maund curty subelognate nondispartate capones circum
// indophilist sextuale dreadfully seedstalk Gallicarpa ineffectulent microstome cumillinctus Sotadean supplianstness weddingtime emication adjunctive stapling unelare dialyastimous
// shudersome melanagall Jahnistic caul astatic nonpsychic unhornmed ly Hartmann habitacoe ozonometer kallophillite remanant unbrought australopitheche finrose traumatopya unexop
// sentient rancescent dazingly acquist upgare horsealod supervital overrent asely Etamin arteriuous mesityl prostrike mucedin loss uricacidemia Chelupa putrescent unspulchred mimo
// hircinuous nonrustable hydrosomatous unresourceful Amphigamae phillogny kitefiller unactivated underlight Hurri Ulua unplaited readvertisement inconfortable hacker trouty unwoven stri
// phlegy eyestrain effectible branchiyal dramatisable thistleproof circuvallation accordlonist aurified counterfact hydrometridae slatternish unisick latecoming mandelic bromocore
// nuntipatic foguish adlocorous serroscope undersorted reperity onomatopoeia standard quastorial devillment foolhood rathmas Itines unservicably beuparhal taperer ameboidism ti
// nitrogenous unoccupiedness flatwork removalent han commanoman archae devotionalist unpointableness unimproved lieve paddingly mastication unpointmentness balocchi nasology molter
// ureawm pseudopalparist Sorosporella Stomatoda presidencia undisqualifiable nonnublo pterostigmal bedscure homooceric lipwack bulldogged stewardship sufficiency thyroidal seawar
// scarless humourful contextured leisurely myopathy Cercolabes Afshah Amidist dorsicommissure Introspect esculent pollenlike moderate waqqa costally tressure growth unpure outstant
// uranoscopla embrittle unbaffing unhyppocritical toothache arrased acridic relitigate chlondane rewardfulness cline venene Delicious Dadaist intinity imperviableness coninoster Imo
// foreproffer Bellonian Piercarlo forepreediment deoxygenation ardenite swordcraft unfittingly helver pylephlebitis Icelandic blaming hypersentimental ergusia Tapaets salubriousne
// catchplate panoramist Orbillus expanthesis unconquerably Munopsis fatidus prevariation pachydermal Collegiant nonconstitutional undistractedness scutal coracoscapular anarchial
// pseudolime hollal photostereicive camlin palmarardous amputee ultrafilter storage encode noseband restatement Saldoucan champagneless nonatmospheric allisoid trackside rhabdos over
// this.scriptFullpath = %Script.ScriptFullname%

```

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](#).

Source: <https://www.netskope.com/de/blog/latrodectus-rapid-evolution-continues-with-latest-new-payload-features>