POLIZEI
Nordrhein-Westfalen
Dortmund

Schadsoftware / Malware

Quelle: adobe stocks (Polizei NRW)

Gefahren durch Schadsoftware

POLIZEI
Nordrhein-Westfalen
Dortmund

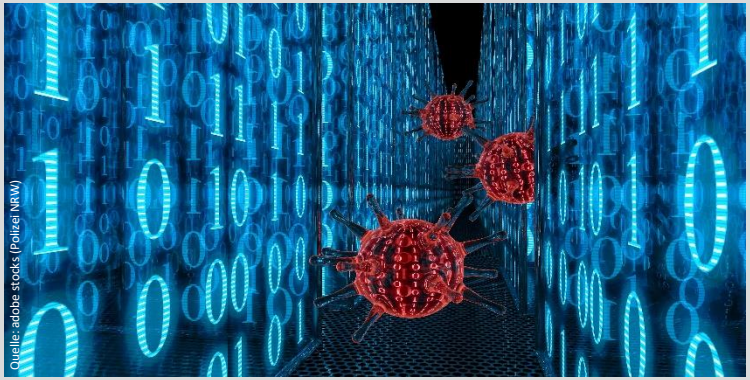
Schadsoftware wird auch als "Malware" bezeichnet, ist eine Abkürzung für "bösartige Software" und der Oberbegriff für alle bösartigen Programme oder Codes.
Derartige Software dient nur dem Zweck, Computer, Computersysteme, Netzwerke, Tablets und Mobilgeräte auszuspionieren, zu übernehmen, zu verschlüsseln, sie zu schädigen oder ganz außer Gefecht zu setzen.
Es gibt verschiedenste Arten von Schadsoftware, die u.a. eingesetzt wird, um durch erzwungene Werbung (Adware) Gewinne zu erzielen, sensible Daten zu stehlen (Spyware), Geld zu erpressen (Ransomware) oder per E-Mail Spam zu verbreiten (Botnetze).

Jeder Betroffene sollte sich direkt an die Polizei wenden!

Quelle: adobe stocks (Polizei NRW)

Viren und Würmer

Ein Softwarevirus benötigt ein Wirtsprogramm und infiziert ein voll funktionsfähiges Programm oder System. Als Folge der Infektion führt dann das befallene Wirtsprogramm bei jedem Aufruf die Aktionen des Schadcodes aus. Die Anwenderinnen und Anwender bemerken oft nichts von den Schadcode-Aktionen im Hintergrund, da das Programm wie gewohnt zu funktionieren scheint. Das Virus kopiert dabei seine digitale DNA in andere Programmdateien hinein. Sobald eine infizierte Datei per Download oder auf anderem Wege auf ein fremdes Endgerät übertragen und dort ausgeführt wird, setzt sich die Infektionsausbreitung systemübergreifend fort.



Anders als Viren kommen Würmer ohne Wirtsprogramm aus. Es handelt sich hier um eigenständig lauffähige Schadprogramme, die sich unter unauffälligem Namen in den Tiefen des Betriebssystems verbergen und ohne dem Zutun des Benutzers aktiv werden. Wenn der Wurm aktiv ist, durchsucht dieser zum Beispiel die Kontaktordner auf dem System, um sich zu reproduzieren und als Anhang an alle gefundenen E-Mail-Adressen zu versenden. Öffnet der Empfänger das Programm im Anhang, wird der reproduzierte Wurm auch auf das neue System übertragen und kann dort ebenfalls Daten und Dateien zerstören.

Viren und Würmer sind die typischen Werkzeuge für breit gestreute und ungezielte Cyber-Angriffe. Hier geht es hauptsächlich darum, möglichst viele Geräte zu infizieren. So können beispielsweise gekaperte Systeme durch das eingeschleuste Schadprogramm ferngesteuert und in ein Botnetz zwecks weiterer krimineller Nutzung integriert werden.

Trojaner und Ransomware

Trojaner zählen zu den gefährlichsten Arten von Schadsoftware und kommen häufig in fingierter Software vor, die von Cyberkriminellen manipuliert wurde. Sie sind häufig als nützliches Programm getarnt und warten darauf, dass arglose Nutzerinnen und Nutzer sie eigenhändig installieren.

Anders als bei Viren und Würmern, verfügen Trojaner über keinen Mechanismus zur Selbstreproduktion. Stattdessen ist die Täuschung ihre Verbreitungsstrategie. Sobald ein Trojaner den Weg auf ein infiziertes System gefunden hat, erhalten die Cyberkriminellen unbefugten Zugriff auf den kompromittierten Computer. Ab diesem Zeitpunkt kann der Trojaner beispielsweise für den Diebstahl von Finanzdaten oder das Einschleusen von weiteren Bedrohungen wie Viren oder Ransomware eingesetzt werden.

Das Wort Ransomware setzt sich aus den Wörtern „ransom“, dem englischen Wort für Lösegeld, und „ware“, die Bezeichnung von verschiedenen Arten von Computerprogrammen zusammen. Ransomware wird oft auch als Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner und Verschlüsselungstrojaner bezeichnet, da diese Schadprogramme den Zugriff auf Daten und Systeme einschränken oder ganz unterbinden können.
Dabei wird meistens nach Befall des Systems der Zugriff blockiert, der Inhalt verschlüsselt und eine Lösegeldsumme erpresst. Das System bzw. die Nutzerdaten werden meistens erst nach Zahlung einer Lösegeldsumme wieder freigegeben. Die Zahlung ist allerdings keinerlei Garantie für die Freigabe der verschlüsselter Daten oder der gesperrten Systeme. Betroffene sollten hier unverzüglich Anzeige bei der Polizei erstatten. Für den Fall eines Angriffs ist es daher immer ratsam, regelmäßig Sicherungskopien herzustellen, um auch ohne Lösegeldzahlung die Datenbestände rekonstruieren zu können.

Adware und Spyware

Der Begriff Adware leitet sich aus dem englischen „Advertisement“ ab, was so viel wie Werbung bedeutet.
Adware wird meistens durch Freeware und kostenlose Shareware auf die Rechner geladen, wobei der Download neben dem gewünschten Programm noch zusätzliche Software zur Anzeige von Werbung enthält. Diese Adwareprogramme können die Browsereinstellungen so verändern, dass sich beim Surfen im Internet plötzlich Pop-up-Fenster mit unerwünschter Werbung auf dem PC, Tablet oder Smartphone öffnen.

Die Grenze von Adware zu Spyware ist hier fließend, wenn zum Beispiel solche Zusatzprogramme heimlich Informationen über Systemkonfigurationen und Surfgewohnheiten erfassen.

Das Wort „Spy“ bedeutet übersetzt Spion. Spyware ist demnach eine Schadsoftware, die die Aktivitäten des Nutzers unbefugt überwacht und an den Autor der Software weiterleitet.

Durch den in der Wirtschaft ständig wachsenden Bedarf an ausspionierten Nutzerdaten, lässt sich mit jedem Seitenaufruf im Web ein immer genaueres Verbraucherprofil erstellen. Daher ist es ratsam, die Vorteile und Risiken bei allen Software-Downloads sorgfältig gegeneinander abzuwägen. Hier stellen Ad-Blocker eine wichtige Maßnahme zum Schutz der Nutzerinnen und Nutzer im Internet dar, da sie effektiv vor Angriffen durch Schadprogramme schützen, die über extern eingebettete Werbeeinblendungen erfolgen.


Quelle: adobe stocks (Polizei NRW)

Rootkit und Keylogger

Der Begriff „Rootkit“, auch Administratorenbausatz genannt, ist eine Sammlung von Softwarewerkzeugen und beschreibt Schadprogramme, die PCs infizieren und den Kriminellen erlauben, weitere Programme auf dem System zu installieren und zukünftige Anmeldevorgänge (Logins) zu verbergen. Hierdurch wird ein dauerhafter, unbemerkter Zugriff auf den Computer ermöglicht.
Diese Schadprogramme werden so programmiert, dass sie tief im Betriebssystem versteckt und so von möglichst keiner Sicherheits- und Antivirussoftware entdeckt werden.
Das Rootkit kann auch verschiedene Tools wie etwa Keylogger, Programme zum Passwort- und Kreditkartendiebstahl enthalten, sowie Bots für DDoS-Attacken oder Funktionen zum Abschalten von installierter Security-Software.

Die Rootkits fungieren dabei meist als Backdoors, die dem Angreifer ermöglichen, von der Ferne aus auf den infizierten Computer zuzugreifen und bestimmte Komponenten darauf zu installieren.

Ein Keylogger ist eine Hard- oder Software, welche die Tastaturanschläge des Nutzers erfasst, speichert und diese Daten dann an den Angreifer weiterleitet. Die Cyberkriminellen haben es hier auf Benutzernamen, Kennwörter, PINs sowie auf Kreditkartendaten abgesehen.
Es wird unterschieden zwischen Software-Keylogger, welche sich zwischen Betriebssystem und Tastatur schalten, die Tastendrucke mitlesen und an das Betriebssystem weitergeben, und Hardware-Keylogger, die einen unmittelbaren physischen Zugang zu dem betroffenem Computer erfordern und direkt zwischen Rechner und Tastatur gesteckt werden. Diese Geräte können die ausgespähten Daten speichern und werden später wieder entfernt.

Exploits und Cryptomining

POLIZEI
Nordrhein-Westfalen
Dortmund

Als Exploit wird Code bezeichnet, mit dem Fehler, Schwachstellen und Sicherheitslücken in Computersystemen ausgenutzt werden, um zum Beispiel im Rahmen von Drive-by-Infektionen Schadcode zu verbreiten. Anschließend versucht der infizierte Inhalt, sich in einem Drive-by-Download auf dem betroffenen Computer zu installieren, wodurch die Entwickler des Exploits die Kontrolle übernehmen können.
Exploits können allerdings auch dazu verwendet werden, Schwachstellen zu erkennen, zu bewerten und die Wirksamkeit von Workarounds und Patches zu überprüfen.

Cryptomining, umgangssprachlich auch als Cryptojacking oder Drive-by-Mining bezeichnet, ist eine mittlerweile immer häufiger auftretende Schadsoftware, die durch einen Trojaner installiert wird und Kriminellen die Möglichkeit erlaubt, den infizierten Computer und dessen Leistung für das Schürfen von Kryptowährung, zum Beispiel Bitcoin, zu verwenden. Das „geschürfte“ Geld senden die Cryptominer dann auf ihr eigenes Konto.

Wie kann man Malware erkennen?

POLIZEI
Nordrhein-Westfalen
Dortmund

Schadsoftware lässt sich durch viele verschiedene und abweichende Verhaltensmuster erkennen.
Achten Sie auf die folgenden verräterischen Anzeichen als Hinweis darauf, dass Ihr Computersystem
mit Schadsoftware infiziert ist:

- Der Computer wird langsamer; eine der größten Auswirkungen von Schadsoftware ist die Verlangsamung der Geschwindigkeit des Betriebssystems, z.B. beim Surfen im Internet oder beim Verwenden von Applikationen
- Auf dem Bildschirm erscheint eine Flutwelle von unerwarteter Pop-up-Werbung
- Das System stürzt ab, friert ein oder zeigt einen Blue Screen
- Sie bemerken einen unerklärlichen Verlust an Plattenspeicher; wahrscheinlich aufgrund von Schadsoftware, die sich auf der Festplatte versteckt
- Das System zeigt einen starken Anstieg an Internetaktivität
- Die Systemressourcen werden ungewöhnlich stark in Anspruch genommen
- Die Startseite des Browsers ändert sich ohne Ihre Genehmigung; Links leiten Sie an unerwünschte Zielseiten weiter
- Im Browser erscheinen unerwartet neue Symbolleisten, Erweiterungen oder Plug-Ins
- Ihr Antivirenprogramm funktioniert nicht mehr und Sie können es nicht aktualisieren

Wie kann man sich schützen?

POLIZEI Nordrhein-Westfalen Dortmund

Starke Passwörter verwenden

Stark ist ein Passwort, wenn es aus mindestens neun Zeichen unter Nutzung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen besteht. Bitte keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch verwenden und auf keinen Fall an Dritte weiter geben. Es wird empfohlen, für verschiedene Onlinezugänge auch unterschiedliche Nutzernamen und Passwörter zu verwenden. Diese Passwörter sollten auch an geeigneten Stellen und vor Dritten geschützt aufbewahrt werden. Optimal ist auch die Verwendung eines Passwortmanagers mit Schlüsselbundfunktion.

Verwenden Sie keine Passwörter, die in der Vergangenheit schon einmal benutzt wurden und vermeiden Sie die „Passwort merken“-Funktion von Anwendungen im Browser und in Applikationen (Apps). Bevorzugt werden sollten auch Dienste, welche die Zwei-Faktor-Authentifizierung unterstützen.

Privatsphäre schützen

Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben. Ein sorgfältiger Umgang mit seinen Profildaten und Bildern ist unerlässlich.

=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!

[Profilbild, personenbezogene Daten, Freunde-Einstellungen, öffentliche-Daten, Selfies, Likes]

Misstrauisch sein

Bei Anfragen von Unbekannten immer misstrauisch sein! Cyberkriminelle verstecken sich in erster Linie hinter anonymen, gefälschten und unseriösen Profilen. Aus diesem Grund sollte jede Kontaktanfrage immer kritisch hinterfragt und keine sensiblen Daten herausgegeben werden. Auch E-Mails von Unbekannten sollten weder geöffnet, noch sollten Anhänge und Links in keinster Weise angeklickt werden. Hier verbirgt sich oftmals Schadsoftware, mit der Absicht Passwörter zu erbeuten, um weitere, kriminelle Handlungen durchzuführen. Oftmals lassen sich Betrüger auch durch die unkorrekte Schreibweise der E-Mailabsenderadresse, deren Inhalt, falsche Umlaute, kryptische Buchstaben oder anhand der Linkadresse erkennen. Eine sichere Website erkennt man am „**s**“ (secure) in der Kopfadresse bei http**s**://...

Wo gibt es Hilfe?

POLIZEI
Nordrhein-Westfalen
Dortmund

Wenn man Opfer von Cybercrime geworden ist, stehen einem die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.

Quelle: ProPK