Malware auf Windows-Computern

Was Spyware, RATs, Ransomware, Logger und Würmer im System bewirken

Anonymisiert

Abgabetermin: 16.02.2023

Facharbeit | Fach: Informatik

Inhaltsverzeichnis

1 Einleitung

Malware (Schadsoftware) bezeichnet Programme, die unerwünschte oder schädliche Funktionen auf Zielsystemen ausführen. Windows-Systeme sind aufgrund ihrer Verbreitung für Angreifer besonders attraktiv. Diese Arbeit beantwortet drei Leitfragen: (1) Welche wesentlichen Malware-Gattungen existieren und wie unterscheiden sie sich technisch? (2) Über welche Vektoren gelangen Angreifer typischerweise in ein System? (3) Welche Schutzmaßnahmen sind in der Praxis wirksam? Zusätzlich wird ein Experiment in einer isolierten virtuellen Maschine (VM) dokumentiert, in dem ein *Malware-Builder* zum Einsatz kommt. Ziel ist, die Datenerhebung (z. B. Passwörter, Cookies, Screenshots) nachvollziehbar zu demonstrieren und Risiken zu bewerten.

2 Arten von Malware

2.1 Spyware

Spyware ist auf *verdeckte Beobachtung* ausgelegt. Technisch reichen die Fähigkeiten von Keylogging (Abgriff von Tastatureingaben) über *Credential Harvesting* (Browser-Passwörter, Cookies, Autofill-Daten) bis hin zu Webcam- und Screenshot-Capturing. Moderne Spyware nutzt persistente Mechanismen (z. B. Autostart-Keys in der Registry, geplante Tasks) und verschleiert sich durch Code-Packing oder Obfuskation. Das Risiko besteht nicht nur im Datendiebstahl, sondern auch in der Profilbildung (z. B. Gewohnheiten, Standorte), die nachfolgende Angriffe erleichtert.

2.2 RAT (Remote Access Tool)

RATs (*Remote Access Tools*) gewähren *Fernsteuerung* des Systems: Dateibrowser, Command-Shell, Prozess- und Dienstverwaltung, Bildschirm-Streaming, Datei-Exfiltration. Häufig implementiert: *Command-and-Control* (C2) über HTTP(S)/WebSockets, optional *Reverse-Shells* zur Umgehung von NAT/Firewalls. Kritisch ist die *Nachhaltigkeit* des Zugriffs: selbst nach Entfernen einzelner Komponenten können Backdoors verbleiben (z. B. zusätzliche Benutzer, geplante Tasks, Registry-Run-Keys).

2.3 Ransomware

Ransomware verschlüsselt Nutzerdaten (oft per Hybridkryptografie: symmetrisch pro Datei, asymmetrisch für die Schlüsselverteilung) und fordert Lösegeld in Kryptowährungen. Neben *Encryption-at-Rest* existieren Varianten mit *Data Exfiltration* und *Double Extortion* (Veröffentlichungsdrohung). Unternehmen sind besonders gefährdet, da Ausfallzeiten

und Wiederherstellungskosten hoch sind. Selbst Zahlung garantiert keine Wiederherstellung.

2.4 Würmer

Würmer verbreiten sich selbstständig, meist über Sicherheitslücken (*Exploits*) in Diensten oder Protokollen. Im LAN können sie sich lateral bewegen (SMB, RDP, schwache Passwörter). Anders als klassische Viren benötigen Würmer oft kein Host-Programm. Ziel ist häufig das *Aufspannen von Botnetzen* für Spam, DDoS oder nachgelagerte Malware-Kampagnen.

2.5 Logger

Logger (insb. Keylogger) protokollieren Eingaben, Zwischenablage und Fensterfokus. Browserspezifische Logger extrahieren Cookies, Sitzungs-Tokens oder Autofill-Daten. In Kombination mit System- und Hardwareinfos (z. B. GPU/CPU) entsteht ein umfassendes Profil. Übertragung erfolgt typischerweise per HTTP(S), Webhooks oder zu C2-Servern.

3 Infektionswege

3.1 Social Engineering

Angriffe zielen auf den Menschen: Vertrauen aufbauen, Dringlichkeit erzeugen, Autorität imitieren (*„Chef braucht sofort diese Datei“*). Häufig werden harmlose Vorwände genutzt, um das Öffnen von Anhängen (`.exe`, `.scr`, `.lnk`, Office mit Makros) zu erreichen. Ergänzend: präparierte Cloud-Links (z. B. vermeintliche PDFs, tatsächlich SFX-Archive).

3.2 Phishing

Phishing repliziert Login-Seiten (Banking, E-Mail, Shops). Nutzer geben Zugangsdaten ein, die sofort abgegriffen werden. *Credential Phishing* wird oft mit Malware kombiniert (z. B. vermeintliche Sicherheits-Updates). Domain-Spoofing (IDN, Typosquatting) und TLS-Zertifikate erhöhen Glaubwürdigkeit.

3.3 Spam

Massenmails streuen bösartige Links/Anhänge breit. Trotz Spamfiltern genügt ein kleiner Bruchteil unvorsichtiger Empfänger, um Angriffe wirtschaftlich zu machen. Häufig genutzt: Archiv-Dateien (`.zip`, `.7z`) mit passwortgeschützten Inhalten (um Scans zu umgehen).

3.4 Alte Datenträger und Geräte

Gefundene USB-Sticks/Wechseldatenträger sind klassische Vektoren (*„USB-Drop Attack“*). Auch *Dead Drops* (öffentliche Ablage) werden genutzt. Zusätzlich riskant: veraltete IoT-Geräte ohne Updates, die als Einstiegspunkt ins Heimnetz dienen.

4 Schutzmaßnahmen

4.1 Windows Defender

Der integrierte Defender bietet Basisschutz (Signaturen, Heuristik, Cloud-Schutz). Grenzen zeigen sich bei neuen Varianten (*Zero-Day*, *Living-off-the-Land*-Techniken). Trotzdem ist er als *First Line of Defense* sinnvoll, insbesondere mit *SmartScreen*, kontrolliertem Ordnerzugriff und aktuellen Patches.

4.2 Antivirus von Drittanbietern

Seriöse Produkte ergänzen um Sandboxing, bessere Verhaltensanalyse, Ransomware-Rollback. Riskant sind „Scareware“-Produkte, die mit Pop-ups Lockmittel setzen. Grundregel: nur direkt vom Hersteller beziehen; Testberichte kritisch lesen.

4.3 Mehr-Augen-Prüfung (Multi-Scan)

Dienste wie *VirusTotal* prüfen Dateien mit Dutzenden Engines parallel, liefern Hashes, Signaturtreffer, Heuristiken und teils dynamische Analysen. Ergebnisse sind *Indikatoren*, kein endgültiger Beweis. Kombiniert mit Sandboxes (in VMs) erhält man robuste Einschätzungen.

5 Experiment: Malware-Builder in der VM

5.1 Zielsetzung und Aufbau

Ziel war die kontrollierte Ausführung eines öffentlich verfügbaren Malware-Builders, um typische Exfiltrationsdaten zu beobachten. Die Tests erfolgten *ausschließlich* auf einer isolierten Windows-VM (Windows 11 Enterprise Eval) ohne Verbindung zu produktiven Konten. Netzwerkzugriffe wurden protokolliert.

5.2 Erstellung des Stubs

Der Builder generiert eine ausführbare Datei (`.exe`) mit wählbaren Optionen (Fake-Fehlerdialog, Autostart, Defender-Deaktivierung, Icon, Obfuskation). Als Exfiltrations-

Endpunkt wurde ein temporärer Webhook konfiguriert. Der Build-Prozess kompiliert und packt den Payload (Python → Executable).

5.3 Distribution & Ausführung

Zur Simulation eines realistischen Flows wurde die Datei auf einen Filehost hochgeladen und in der VM heruntergeladen. Browser warnen bei *ungewöhnlichen Downloads* (niedrige Reputationswerte); die Datei wurde bewusst manuell bestätigt. Beim Start erschien der konfigurierte Fake-Fehler, während im Hintergrund die Sammlung startete.

5.4 Beobachtete Ergebnisse

Kurz nach Ausführung trafen am Endpunkt strukturierte Daten ein:

- Systeminfos (OS-Version, Benutzername, Hardware),
- Browser-Artefakte (Cookies, Passwörter, Verlauf, Zahlungsdaten sofern vorhanden),
- Desktop-Screenshot,
- ggf. Session-Tokens.

Die Daten wurden als Archiv bereitgestellt; innerhalb fanden sich Text- und JSON-Dateien (z. B. `Passwords.txt`, `Cookies.txt`). Bereits wenige Artefakte genügen, um Konten zu übernehmen (Passwort-Reset, Session-Hijacking).

5.5 Fehleranalyse und Risiken

Auffällig: Webhook-Rate-Limits können dazu führen, dass Mehrfach-Uploads unterdrückt werden. Einige AV-Lösungen löschen den Stub beim Download (Signaturtreffer). Kritisch ist die *Dualhook*-Problematik: Builder sind teils selbst bösartig und leiten Daten an Dritte weiter. Daher: nur in einer VM testen, Netz isolieren, keine echten Logins, Images nach Test verwerfen.

6 Zusammenfassung

Malware ist technisch vielfältig und ökonomisch getrieben. Für Endnutzer ist nicht die perfekte Erkennung entscheidend, sondern das *Risikomanagement*: aktuell halten, misstrauisch bei Anhängen/Links, minimale Rechte, Backups, Mehrfaktor-Authentifizierung, Browser-Credential-Manager kritisch prüfen. Das Experiment zeigt, wie niedrig die Hürden für Datendiebstahl sind und wie wichtig Verteidigung in der Tiefe ist (Patchen, AV, Verhalten, Netzsegmentierung, Backups).

Literatur

[1] Arctic Wolf Networks Inc.: *10 Most Common Types Of Malware Attacks*. Online verfügbar unter: https://arcticwolf.com/resources/blog/8-types-of-malware/, Abruf: 08.02.2023.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Virenschutz und falsche Antivirensoftware*. Archivierte Fassung: https://web.archive.org/web/20210607220805/https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html, Abruf: 08.02.2023.

[3] Google Inc.: *How VirusTotal Works*. Online: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works, Abruf: 02.02.2023.

[4] Smug246: *Luna Token Grabber (Repository)*. Online: https://github.com/Smug246/Luna-Token-Grabber, Abruf: 05.02.2023.

[5] Discord Inc.: *Webhook API Documentation*. Online: https://discord.com/developers/docs/resources/webhook, Abruf: 08.02.2023.