Research Institute
Cyber Defence
Universität der Bundeswehr München

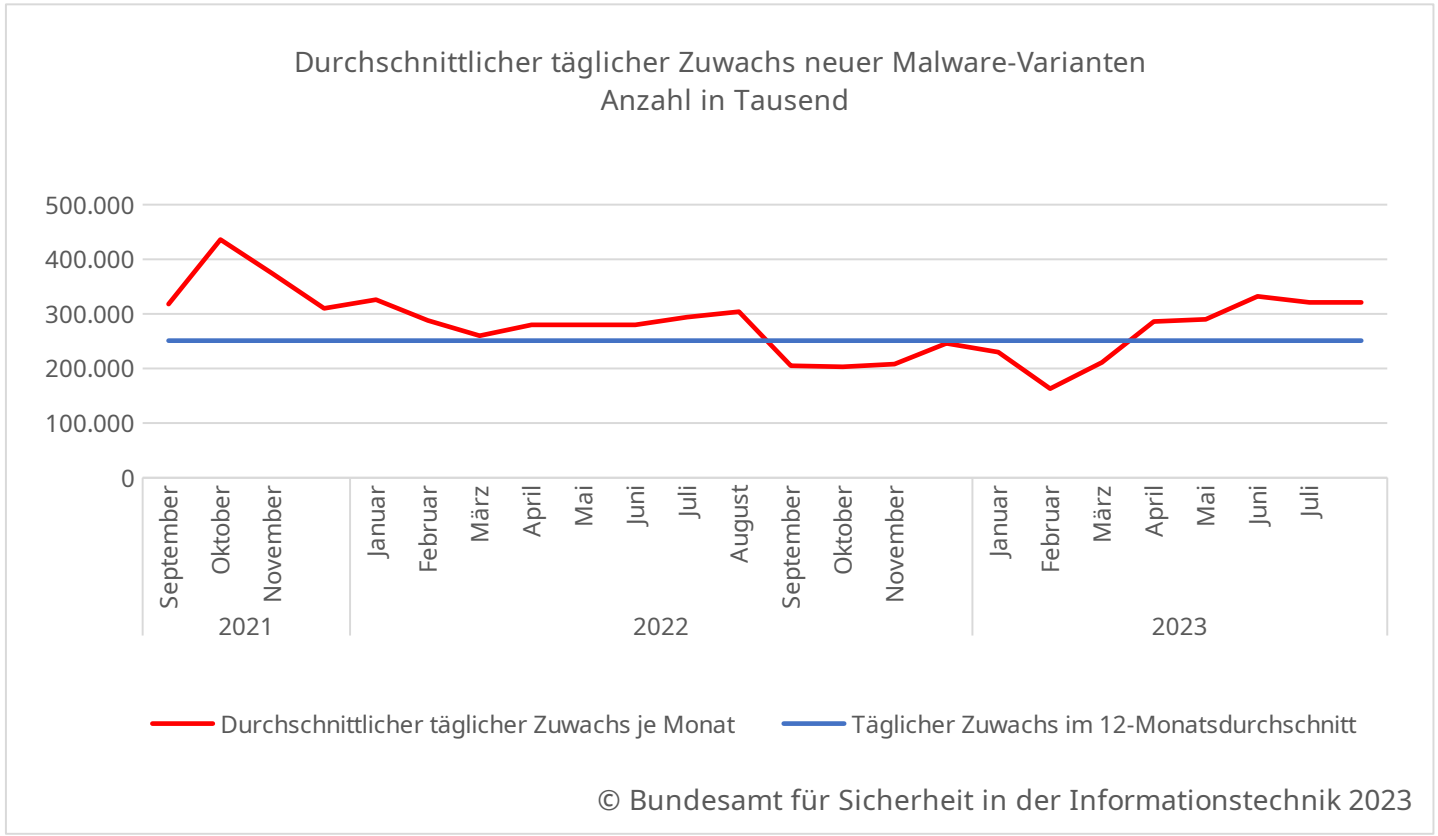
Evaluation of Basic Methods to Bypass Recent Antivirus Systems in Windows Environments

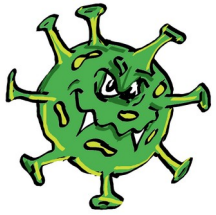
David Maul, Lars Stiemert und Daniela Pöhn

31. DFN-Konferenz “Sicherheit in vernetzten Systemen”

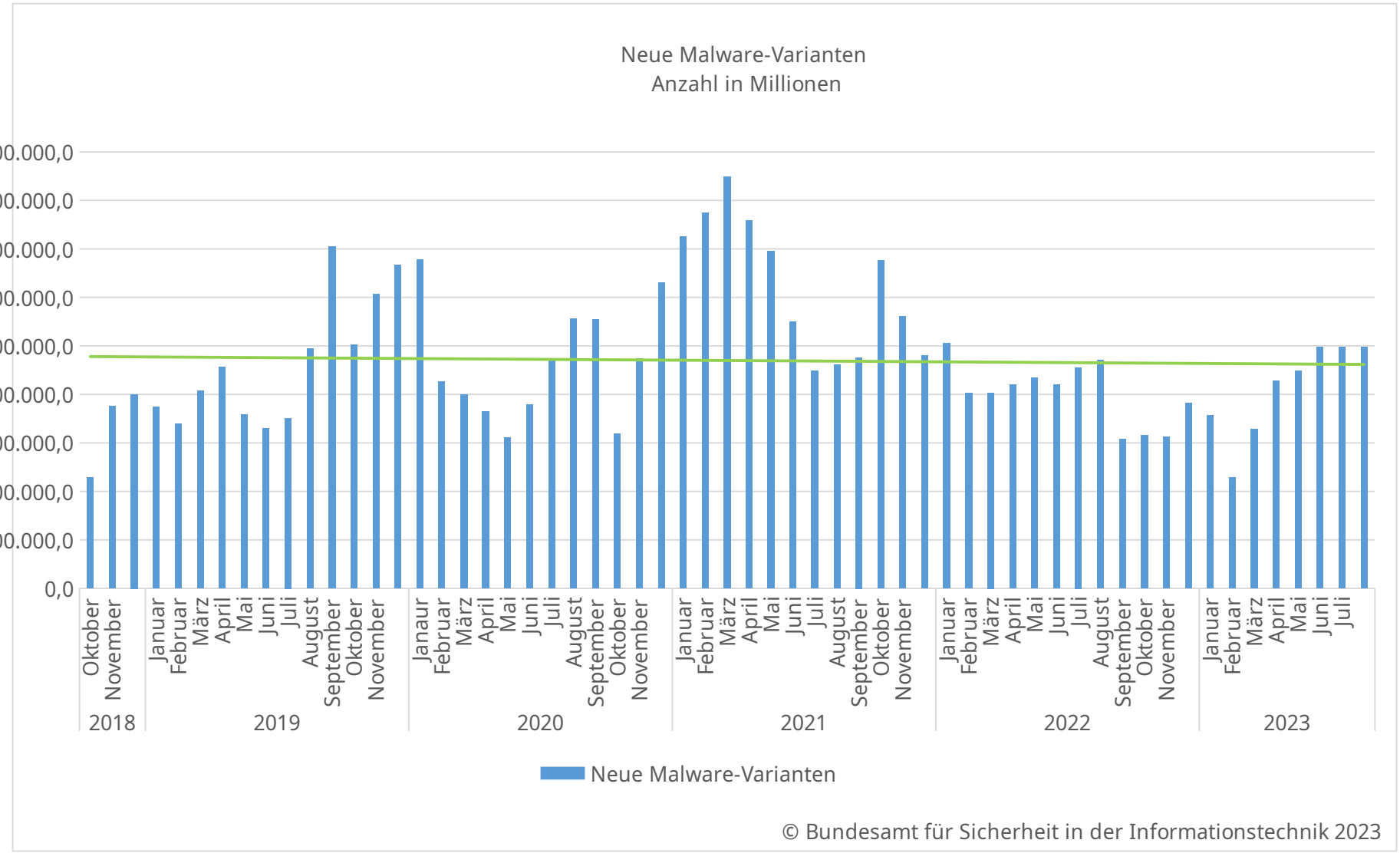
30.-31. Januar 2024, Grand Elysée Hotel Hamburg

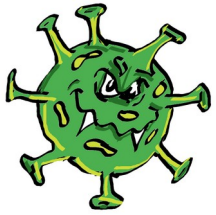
Motivation





Quelle: BSI: Ausgabe 08/2023: Neue Malware- und PUA-Varianten (xlsx)



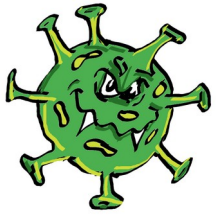


Quelle: BSI: Ausgabe 08/2023: Neue Malware- und PUA-Varianten (xlsx)

Motivation

- Neue Malware-Varianten.
- In den letzten Jahren kamen Techniken wie Packing, Polymorphismus, Deformation und Code-Verschleierung zur Verhinderung der Erkennung durch Antivirensoftware (AV) auf.
- Durch neuartige Technologien und Tools nur geringe bis gar keine technischen Kenntnisse erforderlich, um neue Malware zu erstellen.

Motivation



Quelle: BSI: Ausgabe 08/2023:
Neue Malware- und PUA-Varianten (xlsx)

Art der Malware	Malware		PUA	
	Anzahl in 1.000	Anteil in % der Kategorie	Anzahl in 1.000	Anteil in % der Kategorie
Plattformbezogene Malware				
Plattformen für Desktop-Rechner und Server	7.096	99,2	172	62,0
Windows	7.080	99,8	151	88,2
Windows32	5.234	73,9	142	94,1
Windows64	1.847	26,1	9	5,9
Linux	12	0,2	/	/
MacOS	4	0,1	20	11,6
Plattformen für mobile Geräte	60	2,1	105	38,0
iOS	/	/	/	/
Android	60	99,9	105	100,0
andere	/	/	/	/
Zusammen	7.157	71,8	277	81,6
Plattformunabhängige Malware				
Skript	1.518	54,1	62	99,3
Office	7	0,2	/	/
Java	1	0,1	/	/
Dos	/	/	/	/
Dokumententypen	1.278	45,6	/	/
Zusammen	2.805	28,2	62	18,4

Motivation

- Notwendig, AV-Techniken zu reevaluieren
- Ansatz:
  - 13 AVs in einem kontrollierten Windows-Testbed anhand realer Malware evaluieren
  - Metrik zum Vergleich

Hintergrund – Statische Erkennung

- Signaturbasierte Erkennung: Analysiert die Datei und sucht nach bekannten schädlichen Mustern, der Signatur.
- Heuristikbasierte Erkennung: Sucht nach Heuristiken in einer Datei. Ein solcher Indikator ist z.B., dass die `.text`-Section beschreibbar ist.

Hintergrund – Statische Erkennung

- Unpacking: Dekompromierung nach Einsatz von Packern. Die innere ausführbare Datei ändert ihre Form vollständig, die Semantik bleibt jedoch dieselbe. Die äußere ausführbare Datei extrahiert zur Laufzeit die innere Datei und übergibt die Ausführung.
- Statische Verschlüsselungserkennung: Entschlüsseln oder Erkennen verschlüsselter Malware.

Hintergrund – Statische Erkennung

- X-Raying: Technik zur Aufhebung der Verschlüsselung, z. B. Schlüsselvalidierung (Brute-Force) und invariantes Scannen.
- Emulation: Ausführung der Datei in einer sicheren virtuellen (emulierten) Umgebung. Ermöglicht die spätere dynamische Analyse der Datei und die Prüfung auf schädliche Aktivitäten.

Hintergrund – Dynamische Erkennung

- Verfolgung von Syscalls: Semantik und Reihenfolge von Funktionen, insbesondere von Syscalls, ermöglichen eine Programmanalyse. Abfangen von Aufrufen erfolgt durch das Einfügen von Hooks oder einen Debugger.
- Überwachung der Datenverarbeitung: Aufzeichnen, wie sich der Inhalt bestimmter Speicherorte darauf auswirkt, was später an anderen Speicherorten gespeichert wird.
- Überwachen der Reihenfolge der vom System ausgeführten Maschinenanweisungen: Detaillierte Informationen.

Stand von Forschung und Technik

- Afianian et al. [1]: Klassifizierung für Standard-Evasion-Techniken.
- Rad et al. [7] und Marpaung et al. [27]: Evasion Techniken.
- Kalogranis [20]: Überblick über gängige automatische Tools.
- Vasileios [38]: Umgehung der Entschlüsselung unter Windows XP, Vista und 7.
- Giorgos [18] und Kolbitsch et al. [22]: Spezielle Techniken.
- Perriot und Ferrie [34]: Gegenmaßnahmen.

Zwischenfazit

- Viele Arbeiten konzentrieren sich auf die Theorie hinter einer Technik oder mögliche Gegenmaßnahmen.
- Die Stärke der jeweiligen Methode wird entweder nicht oder nur auf Basis von Shellcode oder VirusTotal gemessen.
- Manche Veröffentlichungen sind älter als fünf Jahre.
- Seitdem hat sich manches geändert.
  → Grundlegende Neubewertung

Methodik - Testumgebung

- Testumgebung
  - VM mit Windows 10 Pro Version 21 und jeweils einer AV Software
  - Ohne Internet: kein Update, aber auch keine zusätzlichen Erkennungsmöglichkeiten
- Malware
  - Ransomware, da hoch-aktiv und visuelle Rückmeldung
  - Auswahl: Maze, Conti, REvil, BlackMatter, Cerber, Crysis, Ryuk, Sage, Virlock und Wannacry

Methodik – AV Software

- Kostenlos:
  - Windows Defender
  - Immunet mit ClamAV engine
- Kommerziell:
  - TrendMicro Maximum Security
  - MalwareBytes Premium
  - Kaspersky Total Security
  - Avira Prime
  - gDataTotal Security
  - BitDefender Total Security
  - McAfee Total Protection
  - Avast Premium Security
  - Vipre Advanced Security
  - McAfee Endpoint Security
  - Sophos Intercept X Advanced mit EDR

Methodik – Evasion Techniken

- Statisch:
  - XOR und ROT Stubs
  - Packing
  - XORing und Packing
  - Fingerprints
  - Code Stalling
- Dynamisch:
  - Remote Thread Injection
  - Safe Mode Malware

Methodik - Metrik

- Basis:
  - Erkennung der Malware
  - 1 Punkt
- Statische Erkennung
  - 2 Punkte
  - Falls erkannt: keine dynamische Erkennung
- Dynamische Erkennung
  - 2 Punkte

Methodik - Limitationen

- Begrenzte Anzahl an Dateien
- Kein Internetzugang

Ergebnisse - Statisch

- XOR und ROT Stubs
  - Liefern vergleichbare Ergebnisse, daher kombiniert
  - Beispiel: WannaCry hat weiterhin den bekannten String `tasksche.exe` im `.rdata` Bereich
  - Allgemein gute Ergebnisse

AV	XOR ROT	
	# Stat	# Dyn
TM	1/5	4/4
WD	8/8	0/0
MB	9/10	0/1
K	3/8	4/5
Aa	8/10	0/2
I	3/7	2/4
GD	10/10	0/0
Bd	10/10	0/0
Mc	6/9	3/3
At	4/7	2/3
V	10/10	0/0
ME	6/9	1/3
SR	10/10	0/0
Dec	88/113	17/25

Ergebnisse - Statisch

- Packing
  - Komprimieren der Malware mit MPRESS
  - Viele AVs detektieren die Malware
  - Dies kann durch Emulatoren, Entpackern oder einem Anstieg der Entropie bei heuristikbasierten Erkennung geschehen.
  - Beispiel: Maze hat eine Entropie von etwa 6,65, komprimiert von etwa 8,00.

AV	Packing	
	# Stat	# Dyn
TM	3/5	2/2
WD	8/8	0/0
MB	4/10	1/6
K	8/8	0/0
Aa	7/10	0/3
I	5/7	1/2
GD	8/10	2/2
Bd	8/10	2/2
Mc	2/9	7/7
At	8/8	0/0
V	8/10	2/2
ME	2/9	4/7
SR	10/10	0/0
Dec	81/114	21/33

Ergebnisse - Statisch

- XORing und Packing
  - Die Kombinationen zeigen Schwachstellen.
  - XORing → Packing: Immunity kann entpacken, aber nicht entschlüsseln.
  - Packing → XORing:
    - Immunet, Trend Micro,
      Malwarebytes, Avira, Avast und Sophos können nicht entschlüsseln.
    - McAfee Total Protection detektiert vier Samples mehr als McAfee Endpoint Security mit dynamischer Erkennung.

AV	XOR → Pack		Pack → XOR	
	# Stat	# Dyn	# Stat	# Dyn
TM	1/4	3/3	0/5	5/5
WD	5/5	0/0	8/8	0/0
MB	4/6	0/2	4/10	2/6
K	3/6	2/3	3/8	4/5
Aa	5/7	0/2	9/10	0/1
I	2/5	2/3	0/7	3/7
GD	4/7	3/3	9/10	1/1
Bd	4/7	3/3	9/10	1/1
Mc	1/7	6/6	2/9	7/7
At	4/6	2/2	1/7	5/6
V	4/7	3/3	9/10	1/1
ME	1/7	3/6	2/9	3/7
SR	7/7	0/0	10/10	0/0
Dec	45/81	27/36	66/113	32/47

Ergebnisse - Statisch

- Fingerprints
  - Schwächen einer rein emulatorbasierten Erkennung wie Windows Defender.
  - GData, Bitdefender und Vipre verwenden einen heuristischen Erkennungsansatz.

Antivirus software	GetCurrentThreadId()
Windows Defender	2612
GData	4
Bitdefender	4
Avast	960
Vipre	4

AV	Fingerprints # Stat	# Dyn
TM	-	-
WD	0/8	7/8
MB	-	-
K	-	-
Aa	-	-
I	-	-
GD	8/10	2/2
Bd	8/10	2/2
Mc	-	-
At	1/7	5/6
V	1/7	5/6
ME		
SR	-	-
Dec	25/45	18/20

Ergebnisse - Statisch

- Code Stalling
  - Jede Erkennung ist heuristisch-basierend.
  - Stalling-Stub selbst hat auch Einfluss auf die Ergebnisse
  - Ergebnis ist gemischt: Teils wird es erkannt, teils nicht.

AV	Code stalling # Stat	# Dyn
TM	0/5	5/5
WD	0/8	7/8
MB	9/10	1/1
K	0/8	7/8
Aa	10/10	0/0
I	0/7	2/7
GD	9/10	1/1
Bd	9/10	1/1
Mc	0/9	8/9
At	1/7	5/6
V	9/10	1/1
ME	0/9	4/9
SR	10/10	0/0
Dec	57/113	42/56

Ergebnisse - Dynamisch

- Portable Executable Injection
  - Evaluation: 32-bit Maze Malware in Windows Media Player (32-bit Programm).
  - Sophos erkennt Hilfsprogramm, aber nicht Malware.
  - Ergebnis ist gemischt: Teils wird es erkannt, teils nicht.
- Safe Mode Malware
  - Malware bootet in den Safe Mode, um das AV System zu deaktivieren
  - Ergebnis:
    - Schlecht
    - Einzig Sophos würde die Malware entdecken, wenn sie diese explizit scannt.

Ergebnisse - Dynamisch

Antivirus software	PE injection		Safe mode	
	Static	Dyn	Static	Dyn
Trend Micro	✗	✔	✗	✗
Windows Defender	-	-	✗	✗
Malwarebytes	✗	✔	✗	✗
Kaspersky	✗	✔	✗	✗
Avira	✗	✔	✗	✗
Immunet	✗	✗	✗	✗
GData	✗	✔	✗	✗
Bitdefender	✗	✔	✗	✗
McAfee Total Protection	✗	✔	✗	✗
Avast	-	-	✗	✗
Vipre	✗	✔	✗	✗
McAfee Endpoint Security	✗	✔	✗	✗
Sophos	✔	-	✗	✗
Detection rate	1/13	9/12	0/13	0/13

✔: detected / ✗: not detected.

Diskussion

- Ergebnis
  - 113 Samples, 66 erkannt
  - Am besten:
    - Windows Defender (43/61)
    - GData (56/65)
    - Bitdefender (67/66)
    - Vipre (53/67).
  - Emulator sehr gut, muss aber kombiniert werden
  - Manche AVs erkennen bekannte Malware, andere sind besser mit den Techniken
- Weitere Arbeiten notwendig

AV	Total			
	# Stat	# Dyn	# all	M
TM	5/24	19/19	24/43	91
WD	29/45	14/16	43/61	147
MB	30/46	4/16	34/62	130
K	17/38	17/21	34/59	127
Aa	39/47	0/8	39/55	133
I	10/33	10/23	20/56	96
GD	47/57	9/9	56/65	177
Bd	48/57	9/9	57/66	180
Mc	11/43	31/32	43/75	161
At	19/43	19/23	38/66	142
V	41/54	12/13	53/67	173
ME	11/43	15/32	26/75	127
SR	47/47	0/0	47/47	141
Dec	362/579	157/217	519/796	

Fazit

- Malware entwickelt sich weiter
  Wie gut erkennt AV Software die hierfür verwendeten Techniken?
  - Letzten Studien mehrere Jahre alt → neue Studie
  - Systematische Evaluation (statisch und dynamisch)
  - Metrik zum Gesamtvergleich
- Zukünftige Arbeiten
  - Größere Studie
  - Internetzugriff
  - Weitere Techniken

Daniela Pöhn
Forschungsinstitut CODE
Universität der Bundeswehr München

daniela.poehn@unibw.de
https://www.unibw.de/code