EUIPO
AMT DER EUROPÄISCHEN UNION FÜR GEISTIGES EIGENTUM

ERMITTLUNG UND ANALYSE VON SCHADSOFTWARE AUF AUSGEWÄHLTEN WEBSITES, DIE MUTMASSLICH URHEBERRECHTE VERLETZEN

ZUSAMMENFASSUNG

September 2018

Kurzfassung

Mutmaßlich urheberrechtsverletzende Inhalte stellen einen erheblichen Verstoß gegen die Rechte des geistigen Eigentums dar. Einige Websites machen solche Inhalte öffentlich zugänglich, teilweise sogar kostenlos und ohne Registrierung. Neben diesen Inhalten verbreiten derartige Websites häufig verschiedene Arten von Schadsoftware (sogenannte Malware) und potenziell unerwünschte Programme (potentially unwanted programs, PUP) und bringen die Nutzer dazu, solche Dateien herunterzuladen und zu starten. Die Studie bietet einen Überblick über aktuelle Beispiele von Malware und PUP auf mutmaßlich urheberrechtsverletzenden Websites. Diese Programme nutzen betrügerische Techniken und sogenanntes Social Engineering – beispielsweise „leere“ Installationen von Spielen oder augenscheinlich „nützliche“ Software –, um die Endnutzer dazu zu bringen, sensible Daten preiszugeben. Im Rahmen der Studie wurde eine ganze Reihe von PUP aufgedeckt, die als „nützliche“ Software, als angebliche Spielinstallationen oder auch als Clients für Video-Streaming-Plattformen getarnt waren. Eine solche Software stellt nicht notwendigerweise eine direkte Gefahr für die Soft- oder Hardware der Nutzer dar. Durch verschiedene Social-Engineering-Tricks kann ein Nutzer jedoch dazu gebracht werden, vertrauliche persönliche Daten oder Kreditkartendetails offenzulegen. Darüber hinaus können auch Informationen über den Computer selbst ohne ausdrückliche Zustimmung des Nutzers an Dritte weitergegeben werden.

Forschungsteam

Das Forschungsteam bestand aus Francesca Bosco, Programmbeauftragte beim Interregionalen Forschungsinstitut der Vereinten Nationen für Kriminalität und Rechtspflege (UNICRI), und Andrii Shalaginov, Doktorand im Bereich Informationssicherheit an der Technisch-Naturwissenschaftlichen Universität Norwegens, Fakultät für Informationstechnik und Elektrotechnik, Institut für Informationssicherheit und Kommunikationstechnologie (Forschungsgruppe Digitale Forensik).

Haftungsausschluss

In diesem Zusammenhang ist darauf hinzuweisen, dass mit der Untersuchung das alleinige Ziel verfolgt wurde, die technischen Eigenschaften der im Rahmen der Studie ermittelten Malware und PUP zu bestimmen, auf die Internetnutzer während der Suche nach mutmaßlich urheberrechtsverletzenden Inhalten stoßen könnten. Die dokumentierten Beispiele für Malware und PUP können nicht als erschöpfend betrachtet werden, und es war auch nicht Ziel der Studie (oder der damit gewonnenen Ergebnisse), die Gesamtwahrscheinlichkeit oder das Risiko einer Infektion mit Malware oder einem PUP zu bewerten, wenn ein Internetnutzer nach mutmaßlich urheberrechtsverletzenden Inhalten sucht.


EUIPO
AMT DER EUROPÄISCHEN UNION
FÜR GEISTIGES EIGENTUM

Vorwort

Mutmaßlich urheberrechtsverletzende Online-Aktivitäten können auf verschiedene Weise finanziert werden, unter anderem über Abonnementgebühren, Spenden, Zahlungen für Zusatzleistungen und Einnahmen aus Online-Display-Werbung.

Allerdings sind nicht alle Finanzierungsmöglichkeiten so harmlos wie die genannten Beispiele. Seit Jahren spielt die Verbreitung von Malware und anderen Arten potenziell unerwünschter Programme (PUP) eine wichtige Rolle bei der Finanzierung mutmaßlich urheberrechtsverletzender Aktivitäten im Internet.

Der durchschnittliche Internetnutzer wird sich der Risiken einer solchen Infektion bei einem Zugriff auf urheberrechtsverletzende Websites oder mobile Anwendungen zunehmend bewusst.

Aus dem IP Youth Scoreboard 2015 (Jugendbarometer 2015 zum Thema geistiges Eigentum) des EUIPO ging hervor, dass 52 % der Jugendlichen die Sicherheit auf einer Website für wichtig erachten, wenn sie auf Online-Inhalte zugreifen. Insgesamt gaben 78 % der Jugendlichen an, dass sie es sich zweimal überlegen würden, wenn sie sich eines Risikos bewusst wären, dass der Computer oder das Gerät mit Viren oder Malware infiziert sein könnte. Insgesamt sagten 84 % der Befragten, dass sie es sich zweimal überlegen würden, wenn sie sich eines Risikos bewusst wären, dass Kreditkartendaten gestohlen werden könnten.

Bei den Recherchen für diese Studie hat sich das Amt eine technisch sehr anspruchsvolle Aufgabe gestellt, nämlich Beispiele von Malware und PUP aufzuspüren und zu dokumentieren, die einem Internetnutzer beim Zugriff auf Raubkopien von beliebten Filmen, Musik, Videospielen und Fernsehsendungen begegnen könnten.

In diesem Zusammenhang ist darauf hinzuweisen, dass mit der Untersuchung das alleinige Ziel verfolgt wurde, die technischen Eigenschaften der im Rahmen der Studie ermittelten Malware und PUP zu bestimmen, auf die Internetnutzer während der Suche nach mutmaßlich urheberrechtsverletzenden Inhalten stoßen könnten. Die dokumentierten Beispiele für Malware und PUP können nicht als erschöpfend betrachtet werden, und es war auch nicht Ziel der Studie (oder der damit gewonnenen Ergebnisse), die Gesamtwahrscheinlichkeit oder das Risiko einer Infektion mit Malware oder einem PUP zu bewerten, wenn ein Internetnutzer nach mutmaßlich urheberrechtsverletzenden Inhalten sucht.

Die Untersuchungen wurden in mehreren Phasen in enger Zusammenarbeit mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol durchgeführt.

Die Ergebnisse zeigen eine Vielzahl verschiedener Malware- und PUP-Bedrohungen, denen ein Internetnutzer begegnen kann, wenn er nach mutmaßlich urheberrechtsverletzenden Inhalten sucht. Der Großteil der dokumentierten Malware und PUP kann als Trojaner oder andere unerwünschte Software bezeichnet werden, die in der Lage ist, sich unberechtigten Zugriff auf die persönlichen Daten von Internetnutzern zu verschaffen. Diese Beispiele werden nicht nur für die Gemeinschaft der Inhaber von Rechten des geistigen Eigentums relevant und von Interesse sein, sondern auch für Durchsetzungsbehörden und nicht zuletzt für die Verbraucher, die besorgt sind, dass ihre personenbezogenen Daten ohne ihre Zustimmung verwendet werden.

Zusammenfassung

Die Studie bietet einen Überblick über aktuelle Beispiele von Malware und potenziell unerwünschten Programmen (PUP) auf mutmaßlich urheberrechtsverletzenden Websites. Diese Programme nutzen betrügerische Techniken und sogenanntes Social Engineering – beispielsweise „leere“ Installationen von Spielen oder augenscheinlich „nützliche“ Software –, um die Endnutzer dazu zu bringen, sensible Daten preiszugeben.

Ziel dieser Studie ist es, bösartige oder anderweitig unerwünschte Software aufzudecken und zu dokumentieren, die über ausgewählte Websites verbreitet wird, die im Verdacht stehen, das Urheberrecht zu verletzen. Anschließend sollen die gefundenen Beispiele anhand verschiedener Malware-Taxonomien kategorisiert werden. In diesem Zusammenhang ist hervorzuheben, dass mit der Studie das alleinige Ziel verfolgt wurde, die technischen Eigenschaften der im Rahmen der Untersuchung ermittelten Malware und PUP zu bestimmen, auf die Internetnutzer während der Suche nach mutmaßlich urheberrechtsverletzenden Inhalten stoßen könnten. Die dokumentierten Beispiele für Malware und PUP können nicht als erschöpfend betrachtet werden, und es war auch nicht Ziel der Untersuchung (oder der damit gewonnenen Ergebnisse), die Gesamtwahrscheinlichkeit oder das Risiko einer Infektion mit Malware oder einem PUP zu bewerten, wenn ein Internetnutzer nach mutmaßlich urheberrechtsverletzenden Inhalten sucht. Für die Zwecke dieser Studie gelten Fernsehsendungen, Filme, Musik und Videospiele als urheberrechtlich geschützte Inhalte.

Ergebnisse der Studie

Mutmaßlich urheberrechtsverletzende Inhalte stellen eine erhebliche Verletzung der Rechte des geistigen Eigentums dar. Einige Websites machen solche Inhalte öffentlich zugänglich, teilweise sogar kostenlos und ohne Registrierung. Neben diesen Inhalten verbreiten derartige Websites häufig verschiedene Arten von Schadsoftware (sogenannte Malware) und potenziell unerwünschte Programme (potentially unwanted programs, PUP) und bringen die Nutzer dazu, solche Dateien herunterzuladen und zu starten. Bei der Suche nach entsprechenden Websites auf Basis der Liste des Unternehmens Alexa Internet Inc. mit den 500 meistaufgerufenen Websites sowie einer Simulation der durchschnittlichen Nutzersuche mit bekannten Suchmaschinen wie Google, Yahoo und Bing wurde festgestellt, dass sich die Liste der Websites zwischen den beiden Runden der Studie verändert hat. Diese Veränderung ist wahrscheinlich auf die Bemühungen der Suchmaschinen zurückzuführen, Links zu mutmaßlich urheberrechtsverletzenden Websites zu entfernen, während gleichzeitig jedoch ständig neue verdächtige Websites hinzukommen. Eine interessante Entdeckung im Rahmen der Suche nach entsprechenden Websites bezog sich auf die Tatsache, dass die überwiegende Mehrheit der Websites in den Vereinigten Staaten gehostet wird oder die Domain-Namen auf einen Server in den USA schließen lassen. Tatsächlich werden nur wenige Websites auf Servern innerhalb der EU gehostet. Zudem sind .com und .net die Top-Level-Domains, die bei mutmaßlich urheberrechtsverletzenden Websites am häufigsten verwendet werden. Das kann daran liegen, dass sich der Nutzer im Gegensatz zu länderspezifischen Top-Level-Domains hierbei nicht mit einem Reisepass oder anderen Identifikationsdokumenten ausweisen muss. Durchschnittlich gesehen, wurden zwischen den beiden Runden zur Ermittlung geeigneter Websites 20 % neue Websites hinzugefügt und 20 % der

vorhandenen Websites entfernt. Außerdem wurden fast 8 % der in beiden Runden ermittelten Websites von der Plattform VirusTotal als bösartig eingestuft. Mithilfe verschiedener Content-Management-Systeme lassen sich mittlerweile ohne großen Aufwand Websites erstellen, um den Nutzern Inhalte – darunter auch bösartige Anwendungen – zur Verfügung zu stellen.

Bevor die Studie sich der Sammlung von Beispielen für Malware widmete, untersuchte sie die Malware-Bedrohungen im Jahr 2017 und zeichnete ein Bild der aktuellen Lage. Diese Erkenntnisse wurden bei der weiteren Analyse von Malware herangezogen, um den allgemein anerkannten Grundsätzen bei der Identifizierung der verschiedenen Malware-Arten und -Familien Rechnung zu tragen. Insgesamt wurden in beiden Runden der Datenerhebung 106 Dateien gesammelt. Dazu zählten Dateien, die direkt von mutmaßlich urheberrechtsverletzenden Websites heruntergeladen wurden, sowie Dateien, die während der Ausführung der heruntergeladenen Dateien erstellt wurden. Im Rahmen der Studie wurde eine ganze Reihe von PUP aufgedeckt, die als „nützliche“ Software, als angebliche Spielinstallationen oder auch als Clients für Video-Streaming-Plattformen getarnt waren. Eine solche Software stellt nicht notwendigerweise eine direkte Gefahr für die Soft- oder Hardware der Nutzer dar. Durch verschiedene Social-Engineering-Tricks kann ein Nutzer jedoch dazu gebracht werden, vertrauliche persönliche Daten oder Kreditkartendetails offenzulegen. Darüber hinaus können auch Informationen über den Computer selbst ohne ausdrückliche Zustimmung des Nutzers an Dritte weitergegeben werden.

Die zusammengestellte Malware wurde zunächst mithilfe von Open-Source-Tools analysiert, um die interne Logik zu verstehen, mögliche bösartige Aktivitäten aufzudecken und deren Relevanz für die vorliegende Malware-Studie zu beurteilen. Neben der Vorabanalyse mit Open-Source-Tools wurden die gesammelten Malware-Beispiele von der EMAS-Plattform (Europol Malware Analysis Solution) analysiert. Dabei wurde eine Vielzahl verschiedener Artefakte und bösartiger Aktivitäten entdeckt. Die EMAS-Berichte enthalten eine umfassende Analyse der Dateien unter Verwendung vier unterschiedlicher Versionen von MS Windows. Dabei wurden Datenverkehr, Funktionsaufrufe und Festplattenaktivitäten zur weiteren Analyse ausführlich protokolliert. Darüber hinaus markiert die Plattform alle verdächtigen Aktivitäten, die während der Dateiausführung erkannt wurden. Nach der Analyse aller Berichte hatte EMAS 35 Arten von bösartigen Aktivitäten festgestellt, die in 17 Klassen von bösartigen Ereignissen eingeordnet werden konnten. Diese reichen von allgemeinen Anomalien (wie dem Starten von Systemprozessen oder der Suche nach Prozessen im Speicher) bis hin zu eindeutig bösartigen Aktionen (wie Keylogger, Rootkit und die Manipulation des Datenverkehrs).

Generell veranschaulichten die zusammengetragenen Binärdateien von Malware und PUP einige unterschiedliche allgemeine Geschäftsmodelle: „nützliche“ Programme in Form eines kostenpflichtigen Abonnements, die angeblich alte Dateien auf dem Computer des Nutzers bereinigen; Simulationen von Spielinstallationen, bei denen der Nutzer seine persönlichen Daten eingeben muss; sowie kostenlose Programme, die Zugang zu Plattformen bieten, die raubkopierte Inhalte verbreiten (z. B. über BitTorrent-Tracker). Beide Runden der Ermittlung geeigneter Websites und der Sammlung entsprechender Malware-Beispiele lieferten vielversprechende Ergebnisse im Hinblick auf das Verständnis der Methoden der Malware-Verbreitung und des Social Engineering bei der widerrechtlichen Beschaffung vertraulicher personenbezogener und identifizierbarer Informationen. Darüber hinaus sind mobile Geräte in den letzten Jahren immer beliebter geworden, was insbesondere an den zahlreichen PUP für das Android-Betriebssystem erkennbar ist, die über Distributionsplattformen mit mutmaßlich urheberrechtsverletzenden Inhalten verfügbar sind. Die vorgenommenen Analysen wurden zueinander in Beziehung gesetzt, und es wurde die Schlussfolgerung gezogen, dass die Bedrohungslandschaft für Malware, die über urheberrechtsverletzende Websites verbreitet wird, ausgefeilter ist, als es auf den ersten Blick erscheinen mag. Einige der entdeckten Softwareprogramme können zusätzlich als Trojaner, Adware, Backdoor und Agent klassifiziert werden. Hinzu kommt, dass außerdem viele spezifische Malware-Familien wie WisdomEyes, DealPly und FileRepMalware gefunden wurden. Darüber hinaus gilt eine solche umfassende Kategorisierung nicht nur für Microsoft Windows, sondern gleichermaßen auch für die Android-Plattform. Die Vermögenswerte der Nutzer sind zahlreichen Bedrohungen ausgesetzt, u. a. dem Diebstahl vertraulicher Anmeldeinformationen, personenbezogener Daten und Informationen zur Hardwarekonfiguration sowie der Manipulation des Datenverkehrs. Auch wenn es sich bei der identifizierten Software um PUP handelt, können sie dennoch Folgen für die Nutzer haben,

insbesondere in Fällen, in denen der durchschnittliche Nutzer nicht umfassend über grundlegende Online-Sicherheitspraktiken und -maßnahmen informiert ist.

Nachstehend findet sich ein Beispiel der Ergebnisse dieser Studie.

Website 03

Die Website bringt die Nutzer dazu, ein vermeintliches Spiel zu installieren; der gesamte Prozess der Beschaffung der vertraulichen Daten eines Nutzers hat sich zwischen der ersten und zweiten Runde der Malware-Sammlung geändert. Der Nutzer dieses Dienstes lädt ein Archiv herunter, dessen Inhalte als spielbezogene Dateien getarnt sind, jedoch keine explizite ausführbare Binärdatei, die von Antivirenprogrammen als bösartig erkannt würde. Das verschlüsselte Archiv gewährt ausschließlich Zugriff auf die Dateinamen, nicht aber auf den Inhalt der Dateien.

Website 09

Die Website bietet Zugriff auf alle Arten von Videoinhalten, die mithilfe eines Software-Tools über Torrent-Tracker abgerufen werden können. Dieses Tool erfordert im Vergleich mit anderen BitTorrent-Trackern weniger Nutzerinteraktionen.
Mit wenigen Klicks können Inhalte aus unbekannten Quellen heruntergeladen werden, wobei der Nutzer weder geschützt ist noch die Kontrolle darüber hat, was heruntergeladen wird.

Website 08

(Android) Die Website bietet Zugang zu einer Reihe kostenloser mobiler Anwendungen ohne Registrierung. Eine Anwendung bietet unbegrenzten Zugriff auf das Streaming von Fernsehsendungen und Filmen. Der Nutzer wird nicht ausdrücklich dazu aufgefordert, vertrauliche Daten oder Zahlungsdetails für den Kauf von urheberrechtlich geschützten Videos anzugeben. Er muss jedoch die Sicherheitseinstellungen deaktivieren, um die Installation von Anwendungen aus anderen Quellen als den offiziellen zu ermöglichen.

Methodik

Zur Durchführung der Untersuchung musste eine fundierte Methodik für die Auswahl der Titel und Websites eruiert werden; außerdem war es technisch anspruchsvoll, die gefundenen Beispiele von Malware und PUP zu erkennen und zu dokumentieren. Im Folgenden wird die angewendete Methodik kurz beschrieben:

1. In Phase I der UNICRI-Untersuchung wurde in Zusammenarbeit mit der Europäischen Beobachtungsstelle für Verletzungen von Rechten des geistigen Eigentums („Beobachtungsstelle“) eine Expertengruppe eingerichtet, die bei der Auswahl der Forschungsmethodik und der für die Analyse zu verwendenden Websites sowie bei der Bewertung der in jeder Phase des Projekts durchgeführten Untersuchungen beratend tätig war. Die Expertengruppe bestand aus Vertretern der Interessenvertreter der Beobachtungsstelle, der Organisationen der Rechteinhaber, der Hochschulen, der Durchsetzungsbehörden und der EU-Agenturen.

2. Parallel dazu wurde das Forschungsteam zusammengestellt. Im Rahmen dieses Berichts war es technisch nicht möglich[1], Beispiele aus allen EU-Mitgliedstaaten zu untersuchen; daher wurden

[1] Die Anzahl der ausgewählten Länder wirkt sich direkt auf die Anzahl der ausgewählten mutmaßlich urheberrechtsverletzenden Websites und der zu analysierenden Binärdateien aus (Anstieg). Daher wurde beschlossen, sich nur auf eine Stichprobe von

in Phase II aus den 28 EU-Mitgliedstaaten zehn Stichprobenländer nach dem Zufallsprinzip ausgewählt.

3. In Phase III wurden beliebte Filme, Fernsehsendungen, Songs und Videospiele ermittelt. Die Beliebtheit der ausgewählten Beispiele bezog sich sowohl auf deren weltweite Beliebtheit als auch auf die Beliebtheit in nur einem oder mehreren der zehn Stichprobenländer am 23. Juni 2017, dem Beginn des Erhebungszeitraums. In den folgenden Phasen der Studie wurden diese Beispieltitel systematisch bei Online-Suchen eingesetzt, um urheberrechtsverletzende Websites und mobile Anwendungen zu finden. Jeder Titel erfüllte zwei oder mehr der folgenden Kriterien:

   - zum Zeitpunkt der Datenerhebung in den EU-Mitgliedstaaten beliebt,
   - zum Zeitpunkt der Datenerhebung auf globaler Ebene beliebt,
   - traditionell beliebt auf globaler Ebene und
   - kategorisiert als Film, Fernsehsendung, Song oder Videospiel.

   Fünf Filmtitel, fünf Fernsehtitel, fünf Musiktitel und fünf Videospieltitel wurden ausgewählt, sodass insgesamt 20 Beispieltitel vorlagen. Es wurde sorgfältig geprüft, welche Quellen herangezogen wurden, um die Beliebtheit eines bestimmten Titels zu ermitteln. Dies machte ein systematisches Auswahlverfahren erforderlich, damit sichergestellt ist, dass die Quelldaten für alle oder zumindest die meisten Mitgliedstaaten verfügbar sind.

4. In Phase IV wurden Websites ermittelt, die im Verdacht standen, illegalen Zugang zu urheberrechtlich geschütztem Material zu ermöglichen, das zum 26. Juni 2017 weltweit und/oder in den zehn Stichprobenländern beliebt war (erste Runde der Sammlung von Malware-Beispielen). In einer späteren Phase der Studie wurden diese Websites auf das Vorhandensein von Malware und potenziell unerwünschten Programmen hin analysiert.

   Die Methodik zur Ermittlung mutmaßlich urheberrechtsverletzender Websites wurde unter Mitwirkung der in Phase I eingesetzten Expertengruppe sowie nach einer Durchsicht der verfügbaren Literatur durch UNICRI entwickelt. Sie wurde speziell dafür entwickelt, eine Stichprobe von Websites zu generieren, die

   - in verschiedenen EU-Mitgliedstaaten beliebt sind, um eine große geografische Abdeckung zu gewährleisten;
   - verschiedene Arten mutmaßlich urheberrechtsverletzender Websites repräsentieren, einschließlich Streaming-Websites, Linking-Websites, Hosting-Websites, Cyberlocker und Torrent-Websites;
   - eine breite Auswahl mutmaßlich urheberrechtsverletzender Inhalte bieten, einschließlich Filmen, Fernsehtiteln, Musik und Videospielen; und
   - Websites repräsentieren, auf die der durchschnittliche Internetnutzer beim Versuch, auf mutmaßlich urheberrechtsverletzendes Material zuzugreifen, stoßen würde.

   Die Auswahl von mutmaßlich urheberrechtsverletzenden Websites erfolgte in fünf Schritten. Die ersten drei Schritte waren darauf ausgerichtet, in den EU-Mitgliedstaaten die beliebtesten Websites zu ermitteln, die im Verdacht stehen, Urheberrechtsverletzungen zu begehen. Diese Methode simulierte solche Szenarien, in denen ein durchschnittlicher Nutzer nach mutmaßlich urheberrechtsverletzenden Websites suchen würde, ohne z. B. den Titel eines Films oder eines Songs anzugeben. Die letzten beiden Schritte zielten darauf ab, mutmaßlich urheberrechtsverletzende Websites zu ermitteln, auf die ein durchschnittlicher Nutzer stoßen könnte, wenn er nach Möglichkeiten sucht, einen bestimmten beliebten Titel herunterzuladen, ohne eine Website anzugeben. Dieser Schritt spielt insbesondere angesichts der Präsenz von mutmaßlich bösartigen Websites eine wichtige Rolle, die Suchergebnisse manipulieren, indem sie versuchen, die Bewertungs-Algorithmen von Suchmaschinen mithilfe von Trendthemen

---

Ländern zu konzentrieren, um den praktischen Teil der Studie innerhalb eines bestimmten Zeitraums erfolgreich durchführen zu können.

positiv zu beeinflussen (Suchmaschinen-Spamming). Zusammen decken die beiden Ansätze die verschiedenen Möglichkeiten ab, die ein durchschnittlicher Internetnutzer verfolgen würde, um mutmaßlich urheberrechtsverletzendes Material online zu finden.

Der Schwerpunkt lag auf der gleichzeitigen Analyse von Malware und PUP speziell für mobile Anwendungen auf Geräten wie Smartphones und Tablets, da diese eine zentrale neue Bedrohung im Bereich der Cyberkriminalität darstellen. Die Analyse wurde auf Android-Geräte beschränkt, da die verfügbare Literatur auf eine stärkere Präsenz von Malware in Android-App-Stores (z. B. Google Play) schließen ließ als im iTunes Store von Apple. Die Methodik wurde dafür entwickelt, eine Stichprobe von mobilen Anwendungen zu generieren, die

- zum Zeitpunkt der Datenerhebung auf globaler Ebene beliebt sind;
- verschiedene Arten von Anwendungen repräsentieren (einschließlich Streaming-Anwendungen, Torrent-Anwendungen und Hosting-Anwendungen);
- eine breite Auswahl mutmaßlich urheberrechtsverletzender Inhalte bieten oder Zugriff darauf gewähren (einschließlich Filmen, Fernsehtiteln, Musik und mobilen Spielen); und
- eine Auswahl dessen darstellen, was dem durchschnittlichen Nutzer eines mobilen Geräts bei dem Versuch begegnet, eine Anwendung herunterzuladen oder zu verwenden, die den Zugriff auf mutmaßlich urheberrechtlich geschützte Inhalte ermöglicht.

5. In Phase V wurden neben mobilen Anwendungen auch Beispiele von Malware und PUP auf den zuvor ermittelten Websites zusammengestellt, die zu einem späteren Zeitpunkt im Hinblick auf die korrekte Kategorisierung näher untersucht werden sollten. Die Phase der Datenerhebung umfasste zwei Runden im Sommer 2017, während derer Beispiele von Malware zusammengetragen und analysiert wurden. Die erste Runde der Erhebung führte zu 1 054 eindeutigen Domänennamen, die zweite Runde zu 1 057 eindeutigen Domänennamen in zehn ausgewählten EU-Mitgliedstaaten. Beispiele für Malware wurden sowohl manuell als auch automatisch zusammengetragen, um die Erfahrung eines durchschnittlichen Nutzers widerzuspiegeln.

Manuelle Erhebung. Bei dieser Methode wurden die in der vorherigen Phase ermittelten Domänen manuell überprüft. Mittels der manuellen Erhebung konnte der zuständige Experte die Erfahrungen eines durchschnittlichen Internetnutzers nachbilden, indem er auf Anzeigen klickte und auf Eingabeaufforderungen auf Websites reagierte.

Automatische Erhebung. Bei dieser Methode wurde ein von einem Experten entwickelter automatischer Webcrawler eingesetzt, der allen vorhandenen Links auf einer bestimmten, mutmaßlich urheberrechtsverletzenden Website folgte. Zunächst sammelte der Webcrawler Informationen über die auf der Startseite der jeweiligen Website enthaltenen Links. In einem zweiten Schritt folgte der Crawler jedem dieser Links zu den damit verknüpften sekundären Websites. Danach folgte er in einem dritten Schritt jedem dieser Links wiederum zu tertiären Websites. In jedem Schritt rief der Webcrawler dabei Binärdateien ab, die für eine anschließende manuelle Analyse von Interesse sein könnten, darunter potenzielle oder mutmaßliche Malware sowie potenziell unerwünschte Programme. Dieser Prozess wurde für bis zu 1 000 Links pro Website fortgesetzt.

6. Sobald die Binärdateien vollständig waren, wurden sie in einem sicheren Rechnerbereich analysiert, um so ihre interne Funktionsweise zu verstehen und eine korrekte Kategorisierung vorzunehmen. Mithilfe von Open-Source-Tools wurde eine Vorabanalyse durchgeführt, um die Ergebnisse zu den Berichten über Cyberbedrohungen in Beziehung setzen zu können. Anschließend wurden die zusammengetragenen Softwarebeispiele zur Analyse an die EMAS-Plattform gesendet; die EMAS-Analyse wurde später mit den Ergebnissen der Vorabanalyse verglichen.

Überblick über die Methodik

Ermittelte Beispiele von Malware und PUP

Bis zum 28. Juli 2017 wurden in der ersten Erhebungsrunde insgesamt 5 240 Websites (1 054 eindeutige Websites) automatisch überprüft, wobei 617 relevante Dateien (Musik-, Video-, Torrent-Dateien und Software) mit einer Gesamtgröße von 47 GB abgerufen wurden. Diese unsortierten Dateien mussten weiter analysiert werden, damit entschieden werden konnte, welche der gesammelten Dateien für die Studie relevant waren. Die Beispiele für urheberrechtsverletzende Websites ähnelten sich in allen zehn Stichprobenländern für jeden Medientyp (Fernsehsendungen, Filme, Musik und Videospiele). Infolgedessen wurde Belgien nach dem Zufallsprinzip aus den Stichprobenländern ausgewählt, und alle in diesem Land ermittelten urheberrechtsverletzenden Websites wurden manuell auf das Vorhandensein bösartiger oder anderweitig unerwünschter Software überprüft. Nach der zweiten Erhebungsrunde lagen am 10. August 2017 insgesamt 3 665 Dateien mit einer Gesamtgröße von 167 GB vor, die automatisch von Websites aus allen Ländern abgerufen worden waren. Bei 1 057 von insgesamt 5 606 Websites aus allen Ländern handelte es sich um eindeutige URLs. Diese Menge machte es unmöglich, alle manuell zu überprüfen.

Nach einer ersten Analyse der gesammelten Dateien wurden aus beiden Erhebungsrunden 106 eindeutige Binärdateien für MS Windows, Android und macOS extrahiert. Konkret handelte es sich um 41 Dateien aus der ersten Runde und 65 Dateien aus der zweiten Runde: zwei für Mac, 15 für Android und 89 für MS Windows. 21 dieser Dateien können als bekannte bösartige Programme betrachtet werden, die auf der Plattform VirusTotal von zahlreichen Lieferanten von Antivirenprogrammen erkannt worden sind. Dazu zählten Dateien, die direkt von mutmaßlich urheberrechtsverletzenden Websites heruntergeladen wurden, sowie Dateien, die während der

Ausführung der heruntergeladenen Dateien erstellt wurden. Anschließend wurden die gesammelten Softwarebeispiele in einer Sandbox-Umgebung analysiert und für eine weiterführende Analyse möglicher bösartiger Aktivitäten an die EMAS-Plattform gesendet. Insgesamt wurden in vier EMAS-Berichten (Windows 7 SP1, Windows 7 SP1 64 Bit, Windows 10 64 Bit, Windows XP SP3) für alle Binärdateien 821 eindeutig bösartige Vorfälle entdeckt. Einige der Berichte enthielten keine verdächtigen Aktivitäten, und einige nannten bis zu zehn bereits bekannte bösartige Aktivitäten. In der letzten Phase der Studie wurden die Ergebnisse der Vorabanalyse und die Ergebnisse aus den EMAS-Berichten zueinander in Beziehung gesetzt. Die quantitative Zusammenfassung der Ergebnisse ist der folgenden Tabelle zu entnehmen.

	Runde 1	**Runde 2**
Datum	28. Juli 2017	Donnerstag, 10. August 2017
In zehn EU-Mitgliedstaaten ermittelte Websites	5 240	5 606
Eindeutige Websites	1 054	1 057
Relevante Dateien	617	3 665[2]
Größe der relevanten Dateien in GB	47	167
An EMAS gesendet		
Android	3	12
macOS	2	–
MS Windows	36	53
Gesamtgröße in Byte	175 600 117	522 991 095

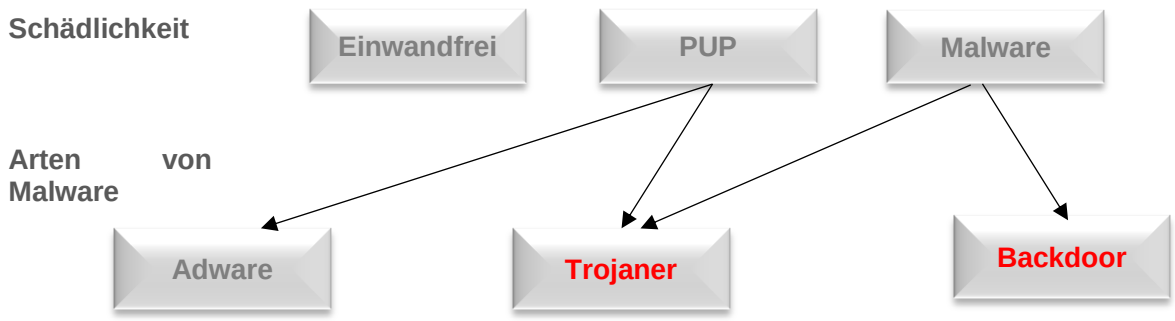
Europol Malware Analysis Solution (EMAS)

Bei der Europol Malware Analysis Solution (EMAS) handelt es sich um eine dynamische, automatisierte Lösung zur Analyse von Malware, die den EU-Mitgliedstaaten von Europol zur Verfügung gestellt wird. EMAS bietet die Möglichkeit, Analyseberichte zu erstellen; die ambitionierteste Funktion dieser Lösung ist jedoch die Zusammenstellung von Informationen für Polizeiermittler. Automatisierte Gegenkontrollen können Verbindungen zwischen Angriffen aufzeigen, die in verschiedenen Ländern mit derselben Malware oder durch dieselbe kriminelle Organisation ausgeführt werden, die hinter einer bestimmten Malware-Familie steckt, und bei denen eine Verbindung zu den gleichen Domänen erfolgt, die im Rahmen verschiedener Ermittlungen innerhalb oder außerhalb der EU untersucht werden. Im Jahr 2015 wurde

Wie aus der nachstehenden Abbildung hervorgeht, lassen sich die gesammelten Binärdateien in der Regel nach ihrer Schädlichkeit als harmlose Dateien (Dateien, die keinen Schaden anrichten), PUP und schädliche Malware kategorisieren. PUP wurden zudem nicht nur im Zusammenhang mit Microsoft Windows entdeckt, sondern auch für Android und macOS, was darauf hindeutet, dass die Entwickler von Malware versuchen, über verschiedene Plattformen so viele Nutzer wie möglich zu erreichen. PUP und Malware können anhand der Hauptarten von Malware, d. h. Trojaner, Adware und Backdoor, weiter differenziert werden. Der größte Teil der gefundenen Software fiel in die Kategorie der PUP. Bei PUP können folgende Geschäftsmodelle zum Einsatz kommen: vermeintliche Spielinstallationen, bei denen persönliche Daten und Kontodaten angegeben werden müssen, das Herunterladen „nützlicher“ Programme, die den Nutzer dazu nötigen, die kostenpflichtige Version in Form eines Abonnements zu erwerben, oder die Installation von kostenlosen Programmen, um auf urheberrechtsverletzende

[2] Die Unterschiede bei den Zahlen in der ersten und zweiten Runde lassen sich dadurch erklären, dass die automatische Erhebung in der zweiten Runde Websites umfasste, die auf jeder ihrer Webseiten mehrere Sätze von Dateien enthielten.

Plattformen zuzugreifen. Diese Anwendungen können eine Gefahr für die persönlichen Daten und die Computerkonfiguration der Nutzer darstellen. Durch Social-Engineering-Tricks können auch verschiedene Arten von privaten Daten, wie z. B. Kreditkartendetails, personenbezogene Informationen und Zugangsdaten zu Social-Media-Konten, offengelegt werden. Im Rahmen der Untersuchung wurden außerdem 15 Android-Anwendungen auf Drittmärkten ermittelt, und nach der Vorabanalyse wurde der Schluss gezogen, dass solche Anwendungen bei der Verbreitung von urheberrechtsverletzenden Inhalten und der Offenlegung personenbezogener Daten eine Rolle spielen können.



Gefahren für Endnutzer

In den beiden Runden, in denen die entsprechenden Websites ermittelt und die aufgedeckte Malware analysiert wurde, wurden keine Ransomware-Binärdateien gefunden. Generell kann der größte Teil der gefundenen Malware als Trojaner eingeordnet werden. Das bedeutet, dass sie auf den Websites als harmlose, häufig verwendete oder beliebte Software dargestellt werden, während sie in Wirklichkeit private Informationen stehlen oder offenlegen. Ein unerfahrener Nutzer setzt möglicherweise ein hohes Maß an Vertrauen in die Software und ist nicht in der Lage, etwaige Unregelmäßigkeiten zu erkennen. Darüber hinaus können statische Programmanalysen und dynamische Verhaltensbeobachtungen in Bezug auf eine solche Software ohne Zugang zum Quellcode nicht die gesamte Funktionalität aufzeigen. Im Anschluss an eine vorläufige Analyse der gefundenen Malware offenbarte die EMAS-Analyse weitere spezifische bösartige Aktivitäten. Die Installation einer solchen Software auf dem Computer eines Endnutzers kann beträchtliche Folgen haben: Neben finanziellen Verlusten besteht auch das Risiko des Diebstahls persönlicher Daten und des unberechtigten Zugriffs und der Kontrolle. Diese Aktivitäten können dazu führen, dass persönliche Daten offen oder in verschlüsselter Form abgeschöpft und an Dritte weitergegeben werden. Dabei kann es sich beispielsweise um Kontoinformationen handeln, die im Browser gespeichert sind, um Angaben zur Hardware- bzw. Softwarekonfiguration des Computers oder grundsätzlich um alle Informationen, die über die Tastatur eingegeben werden.

ERMITTLUNG UND ANALYSE VON SCHADSOFTWARE AUF AUSGEWÄHLTEN WEBSITES, DIE MUTMASSLICH URHEBERRECHTE VERLETZEN

ZUSAMMENFASSUNG

September 2018