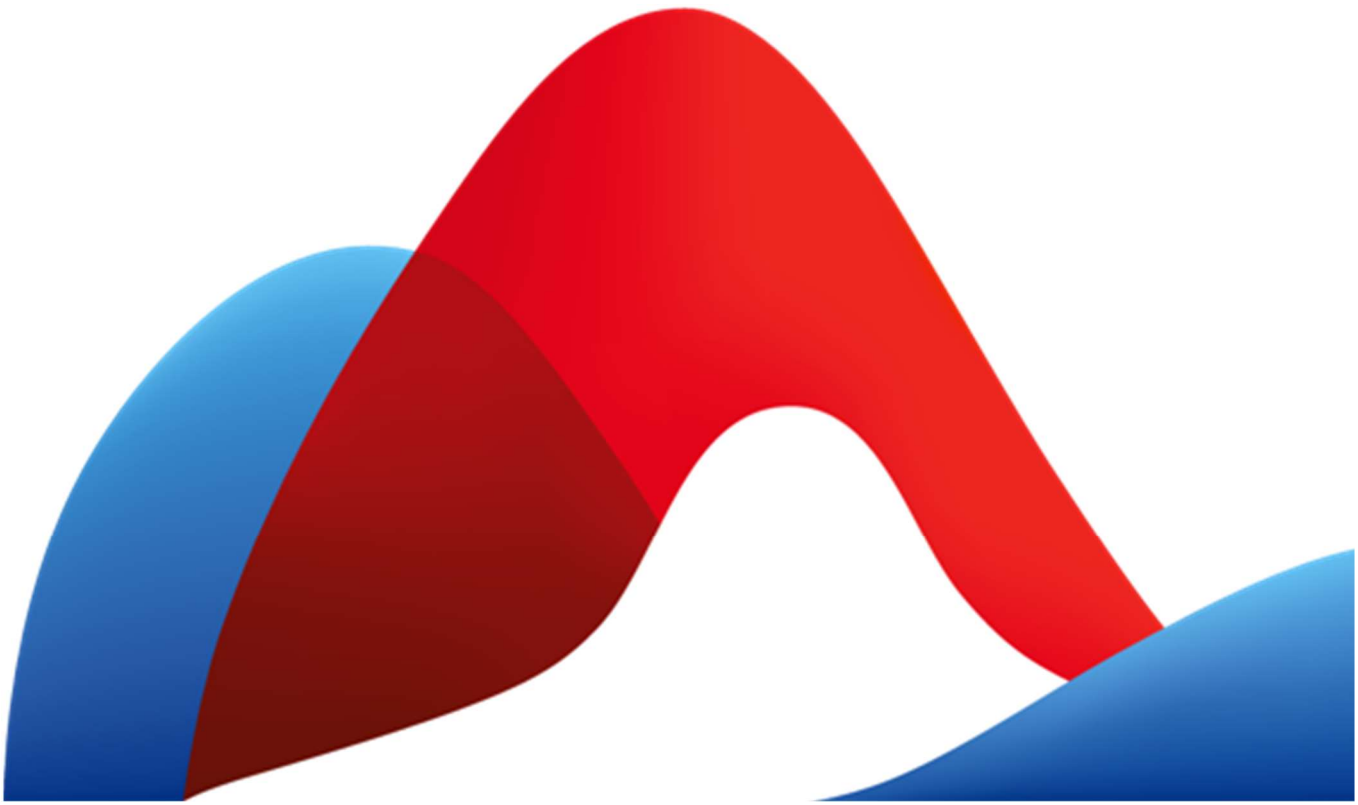
Cyber Security 2018:

Artificial Intelligence, Malware & Cryptocurrencies

Autor: Swisscom Security

Dieser Report wurde durch die enge Zusammenarbeit zwischen Swisscom Security mit weiteren Betriebseinheiten realisiert.

Mai 2018



Inhaltsverzeichnis

1. Einleitung ... 3

2. Lagebild – Bedrohungsradar ... 4

2.1 Methodik ... 4
2.2 Bedrohungen ... 5
2.3 Fazit ... 8

3. Artificial Intelligence & Cyber Security ... 10

3.1 Interview mit Laure Willemin, Head of AI, Swisscom ... 10
3.2 Anwendungen von AI & ML in der Cyber Security ... 12
3.3 Fazit ... 14

4. Bedrohungen im Swisscom Netz ... 15

4.1 Malware Call Home ... 16
4.2 Crypto Mining ... 19
4.3 Fazit ... 21

5. Glossar ... 23

1. Einleitung

Der Cyber Security Report von Swisscom geht 2018 in sein zweites Jahr. Neben der Bedrohungslage betrachten wir zwei Themen, die die Security-Community innerhalb Swisscom, bei unseren Partnern und Kunden, aber auch international aktuell besonders beschäftigen.

Erstens: die Anwendung von künstlicher Intelligenz im Security-Umfeld. Hier sehen wir einerseits den missbräuchlichen Einsatz, um intelligentere Angriffe durchführen zu können. Andererseits aber vor allem den sinnvollen Einsatz, um Angriffe und Schwachstellen schneller und genauer identifizieren und beheben zu können.

Zweitens: die Malware, die wir in unserem Netz identifizieren konnten. Die Verbreitung von Malware ist und bleibt das wichtigste Werkzeug von Angreifern, um Services zu kompromittieren, Daten zu stehlen oder fremde Systeme zu missbrauchen. Die meisten Attacken erfolgen übrigens aus finanziellen Motiven. Somit ist es auch nicht verwunderlich, dass auch Crypto-Währungen in unserem Report ihren Platz finden.

Dieser Report ist als Gemeinschaftsarbeit mehrerer Abteilungen innerhalb von Swisscom erstellt worden.

Für die eilige Leserin, den eiligen Leser, haben wir nach jedem Hauptkapitel jeweils ein Fazit verfasst, das der schnellen Information dient. Folglich verzichten wir in dieser Ausgabe aber auf ein Gesamtsummary am Ende des Reports.

Swisscom hat im vergangenen Februar darüber informiert, dass im Herbst 2017 Unbekannte via einen Vertriebspartner unrechtmässigen Zugriff auf die Angaben von Swisscom Kunden erlangt haben. Dieser Vorfall ist nicht Teil dieses Reports. Mit dem Report wollen wir allgemeine Trends und Tendenzen in der Schweizer Cyberwelt aufzeigen und nicht einzelne konkrete Vorfälle diskutieren. Intern haben wir die Schutzmassnahmen erhöht, um einen erneuten Vorfall der erwähnten Art ausschliessen zu können.

2. Lagebild – Bedrohungsradar

Der Ursprung von Bedrohungen findet sich in der stetigen Entwicklung neuer Technologien und deren Anwendung und Verbreitung in der Gesellschaft. Potenzielle Bedrohungen müssen frühzeitig erkannt und systematisch erfasst werden. Um die Bedrohungslage und deren Evolution abzubilden, verwenden wir einen Radar (Abbildung 1).

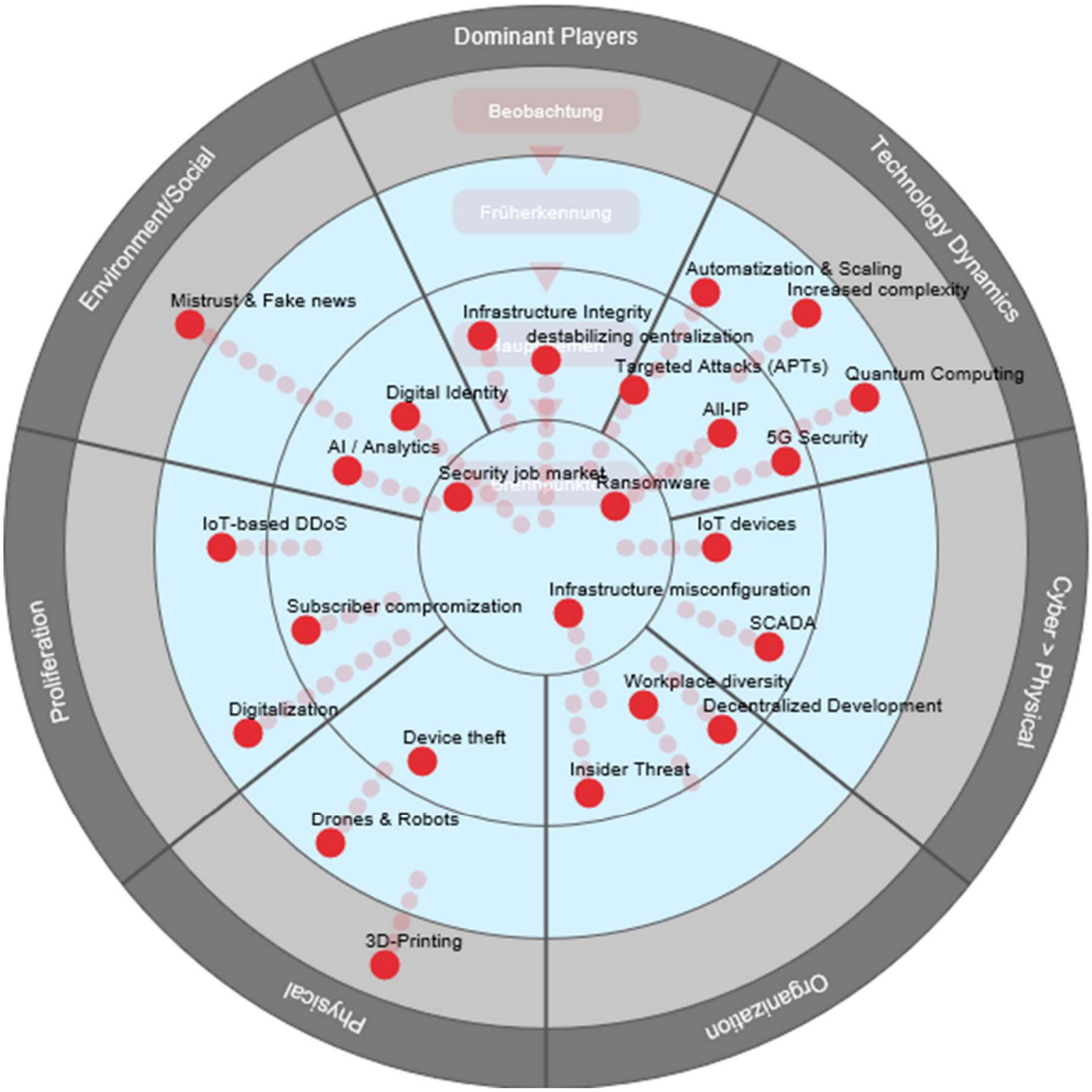


Abbildung 1: Bedrohungsradar

2.1 Methodik

Der Bedrohungsradar ist in sieben Segmente unterteilt, die die unterschiedlichen Domänen der Bedrohungen voneinander abgrenzen. In jedem Segment können die dazugehörenden Bedrohungen in einem von vier konzentrischen Kreisen zugeordnet werden. Die Kreise zeigen die Aktualität der Bedrohung an und damit auch die Unschärfe, die in der Beurteilung der Bedrohung liegt. Je näher zum Kreismittelpunkt

die Bedrohung verortet ist, desto konkreter ist sie und umso wichtiger sind angemessene Gegenmassnahmen. Die Kreise kennzeichnen wir als

- **Brennpunkte** für Bedrohungen, die bereits real sind und mit relativ grossem Einsatz von Ressourcen bewältigt werden.
- **Hauptthemen** für Bedrohungen, die bereits vereinzelt eingetreten sind und mit normalem Ressourcen-Einsatz bewältigt werden. Oft bestehen geregelte Prozesse, um derartigen Bedrohungen effizient zu begegnen.
- **Früherkennung** für Bedrohungen, die noch nicht eingetreten sind oder aktuell nur sehr wenig Wirkung zeigen. Es wurden Projekte gestartet, um der zukünftig wachsenden Bedeutung dieser Bedrohungen frühzeitig begegnen zu können.
- **Beobachtung** für Bedrohungen, die erst in einigen Jahren eintreten werden. Es gibt keine konkreten Massnahmen für den Umgang mit diesen Bedrohungen.

Weiter weisen die einzelnen, durch benannte Punkte gekennzeichneten Bedrohungen, einen Trend auf. Dieser kann in seiner Kritikalität zunehmend, rückläufig oder stabil sein. Die Länge des Trend-Strahls zeigt die erwartete Schnelligkeit auf, mit der sich die Kritikalität der Bedrohung ändern wird.

2.2 Bedrohungen

2.2.1 Dominant players

Bedrohungen, die von Abhängigkeiten von dominanten Herstellern, Diensten oder Protokollen ausgehen.

Hauptthemen	**Infrastructure Integrity:** In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die System-Sicherheit gefährden. **Destabilizing Centralization:** Starke Zentralisierung in der Struktur des Internets führt zu Klumpenrisiken. Der Ausfall eines Services kann weltweit Auswirkungen haben, wie zum Bespiel bei einem Ausfall von Amazon Web Services (AWS).

2.2.2 Technology dynamics

Bedrohungen, die von der rasanten technologischen Innovation ausgehen und damit einerseits den Angreifern neue Möglichkeiten geben, andererseits durch die Entwicklung selber neue Bedrohungen schaffen.

Brennpunkte	**Ransomware:** Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.

Hauptthemen	**Targeted Attacks (APTs):** Schlüsselpersonen werden identifiziert und gezielt angegriffen, um relevante Informationen zu erhalten oder maximalen Schaden anzurichten. **All-IP:** Im Zuge der flächendeckenden All-IP-Einführung steigen Risiken im Zusammenhang mit der VoIP-Technologie. **5G Security:** 5G ist eine noch junge Mobilfunk-Technologie, die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.
Früherkennung	**Automatization & Scaling:** Stärkere Automatisierung technischer Betriebsprozesse wird bei erfolgreichen Angriffen oder Fehlkonfigurationen grössere Auswirkungen haben. **Increased Complexity:** Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Dadurch steigt die Risikoexposition und wird die Fehlersuche erschwert. **Quantum Computing:** Quantencomputer können bestehende kryptographische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit knacken können.

2.2.3 Cyber goes physical

Angriffe über die Infrastruktur im Cyberspace werden vermehrt Schaden in der physischen Welt verursachen.

Hauptthemen	**IoT Devices:** Schwach geschützte Geräte können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z. B. der Verfügbarkeit oder Datenintegrität eingeschränkt werden. **SCADA:** Es existieren nach wie vor viele schlecht oder gar nicht geschützte Kontrollsysteme für Anlagen der kritischen Infrastruktur.

2.2.4 Organization

Bedrohungen, die von Veränderungen in Organisationen ausgehen oder Schwächen in Organisationen ausnutzen.

Brennpunkt	**Infrastructure Misconfiguration:** Ausnutzung fehlkonfigurierter Infrastruktur-Komponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden.
Hauptthemen	**Workplace Diversity:** Neben den vielen Chancen, die neue Arbeitsmodelle mit sich bringen, führt der unkontrollierte Einsatz solcher Modelle, wie z. B. «Bring your own Device» (BYOD) oder verstärkter Einsatz von Remote-Arbeitsplätzen zu einer grösseren Risiko-Exposition.

	Insider Threat: Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich. **Decentralized Development:** Klassische Entwicklungsabteilungen sterben aus, die Applikations-Entwicklung rückt näher in die Business Units bei gleichzeitig kürzer werdenden Release-Zyklen.

2.2.5 Physical

Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind.

Hauptthemen	**Device Theft:** Der Diebstahl insbesondere von Komponenten der kritischen Infrastruktur oder zukünftig vermehrt von IoT-Geräten kann zum Datenverlust führen oder die Verfügbarkeit der Services beeinträchtigen.
Früherkennung	**Drones and Robots:** Aufklärung oder Angriffe über weite Entfernungen werden einfacher und günstiger.
Beobachtung	**3D-Printing:** Die Herstellung von z. B. Schlüsseln oder anderen physischen Geräten wird mit der besseren Qualität der 3D-Drucker günstiger und einfacher.

2.2.6 Proliferation

Bedrohungen, die von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und Know-how profitieren. Einerseits, weil die Verbreitung zu mehr Angriffsflächen führt und andererseits, weil sie die Verfügbarkeit von Angriffs-werkzeugen erhöht.

Hauptthemen	**Subscriber Compromization:** Schadsoftware greift private Daten der Mobile-Nutzer an oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt.
Früherkennung	**IoT-based DDoS:** Starkes Wachstum bei geringem Schutz von IoT-Geräten führt zu mehr "Übernahme-Kandidaten" für Botnetze. **Digitalization:** Immer stärkere Vernetzung der realen und virtuellen Welt und von Privat- und Geschäftsleben führt zu mehr Angriffswegen.

2.2.7 Environmental / Social

Bedrohungen, die von gesellschaftlich-politischen Änderungen ausgehen oder durch solche Änderungen für Angreifer einfacher oder wertvoller werden.

Brennpunkt	**Security Job Market:** Der Bedarf an Security-Professionals kann nur sehr schwer gedeckt werden, was weniger Know-how im Einsatz gegen immer komplexere und intelligentere Angriffe zur Folge hat.

Hauptthemen	**AI / Analytics:** Mehr Daten und bessere Analysemodelle mittels AI können missbraucht werden, um das Verhalten von Menschen zu beeinflussen. Entscheidungen werden vermehrt autonomen Systemen überlassen. **Digital Identity:** Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z. B. in fremden Namen Verträge zu schliessen.
Beobachtung	**Mistrust & Fake News:** Schwindendes Vertrauen gegenüber staatlichen oder gesellschaftlichen Stellen kann dazu führen, dass der Informationsaustausch zur Identifikation und Abwehr potentieller Angriffe reduziert wird.

2.3 Fazit

Unser Lagebild zeigt, dass die Bedrohungslage komplexer wird. Angreifer profitieren vom steigenden Wert der virtuellen Assets, was die Motivation für einen gezielten und intelligenten Angriff erhöht. Weiter schaffen technologische Innovationen und das Zusammenwachsen der physischen und virtuellen Welt neue Angriffsmöglichkeiten. Gesellschaftliche Veränderungen haben Wirkung auf das Vertrauen untereinander und auf die Art, wie wir zusammen arbeiten. Das können Angreifer für ihre Zwecke nutzen.

Gegenüber dem Lagebild des letzten Jahres können wir feststellen, dass die meisten bekannten Bedrohungen unverändert relevant geblieben sind. Einzelne, wie **Destabilizing Centralization**, **5G Security**, **Insider Threat** und der Einsatz von **Ransomware** sind gegenüber 2017 kritischer geworden. Ursachen dafür können (z. B. im Fall von 5G Security) die stärkere Verbreitung neuer Technologien oder (z. B. Ransomware) die weitere Verbreitung von Werkzeugen sein, um Angriffe durchzuführen.
Die Annahme, dass Bedrohungen über SCADA-Systeme gleich bleiben, haben wir mit einem stärkeren Trend korrigiert. Wir sehen für die Zukunft durch immer weit reichendere Anbindung physischer Systeme an das Internet eine Verschärfung des Problems.
Andere Bedrohungen schätzen wir als weniger kritisch ein. So sehen wir 3D-Printing und IoT-based DDoS-Angriffe in der Realität nicht so häufig wie befürchtet, aber beurteilen sie weiterhin als relevant.

Im Lagebild haben wir auch neue Bedrohungen mit aufgenommen. Diese waren im letzten Jahr bereits bekannt, aber im Gegensatz zu den anderen Bedrohungen als weniger kritisch betrachtet worden. Diese Einschätzung haben wir neu beurteilt. Neu auf dem Radar sind: **Automatization & Scaling, Increased Complexity, Quantum Computing, Decentralized Development, AI / Analytics** und **Digital Identity**. Auffällig dabei ist die technologische Dynamik im Umfeld künstlicher Intelligenz, die einerseits positive Effekte auf die Cyber Security hat, andererseits aber auch die

Bedrohungslage beeinflusst und z. B. potentielle Angreifer mit intelligenten Hilfsmitteln unterstützt.

3. Artificial Intelligence & Cyber Security

Artificial Intelligence (AI)[1], Machine Learning (ML) und Deep Learning beschreiben drei miteinander verwandte Modelle, die wir wie folgt voneinander abgrenzen:

Artificial Intelligence	Artificial Intelligence ist die Intelligenz, welche von Maschinen mit Hilfe von Logik, klaren Regeln und Entscheidungsbäumen dargestellt wird.
Machine Learning	Machine Learning ist eine Untergruppe der AI, die komplexe statistische Techniken verwendet, damit Maschinen Aufgaben mit Hilfe von Erfahrung immer besser erledigen können.
Deep Learning	Deep Learning ist eine Untergruppe von ML, die es der Software ermöglicht, sich selbst zu trainieren, um Aufgaben wie Sprach- und Bilderkennung auszuführen, indem sie einem multiplen neuronalen Netzwerk riesigen Datenmengen bereitstellt.

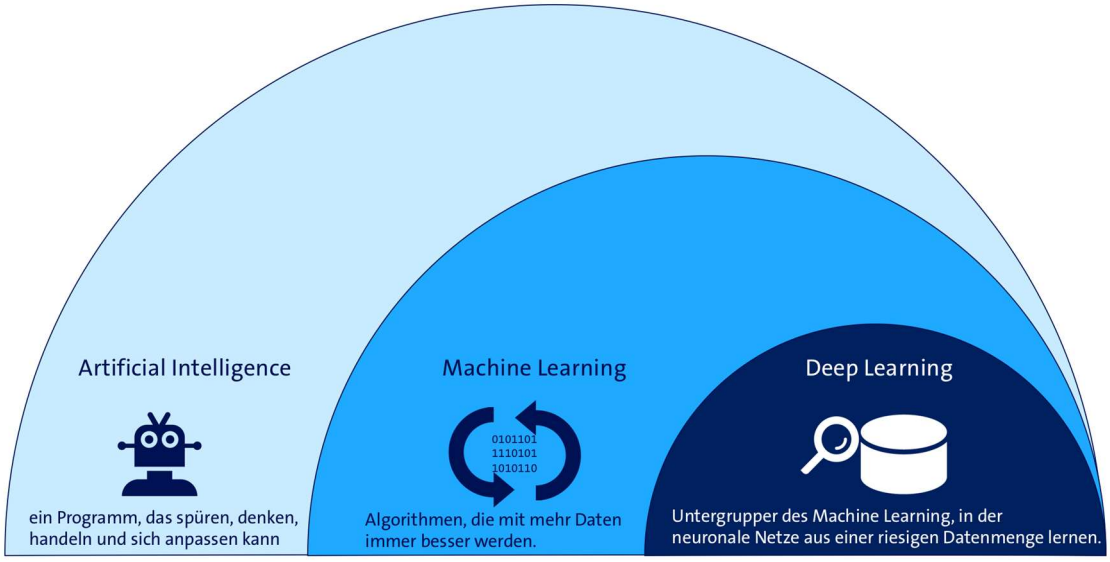


Abbildung 2: Artificial Intelligence, Machine Learning und Deep Learning

3.1 Interview mit Laure Willemin, Head of AI, Swisscom

Laure Willemin und ihr Team entwickeln und betreiben robuste und skalierbare Softwaresysteme unter Nutzung der neuesten Technologien in AI, ML und Deep Learning, unter anderem die Enabler Sentiment Analysis, Key Phrase Extraction, Named Entity Recognition. Unsere Swisscom Kollegin liebt es, sich anspruchsvollen, technologischen Herausforderungen zu stellen, und meistert diese seit über 15 Jahren als Softwareentwicklerin, Systemingenieurin und -architektin.

[1] Im deutschen Sprachraum wird gleichbedeutend von Künstlicher Intelligenz (KI) gesprochen, wobei sich in der Informationstechnologie die englische Bezeichnung durchgesetzt hat und daher hier verwendet wird.

Laure, ist Artificial Intelligence nur eine Chance für Swisscom und unsere Gesellschaft oder sollte sie auch als Sicherheitsbedrohung eingestuft werden?
Wir sehen AI nicht als Bedrohung. Mit der neuen Technologie können wir helfen, grosse Datenmengen besser zu verstehen und die Sicherheitsbemühungen unseres Unternehmens zu unterstützen. Neue Technologien führen oft zu Unsicherheit und Missverständnissen, sie können auch missbräuchlich genutzt werden. Aber die positiven Effekte überwiegen bei Weitem.

Welches sind die häufigsten Missverständnisse, die du bisher über Artificial Intelligence und Machine Learning angetroffen hast?
In erster Linie zu hohe Erwartungen an das, was mit AI möglich ist. Der kritischste Teil eines effektiven Systems sind die Daten. Diese Daten sind oft unstrukturiert und die sie verarbeitenden System müssen trainiert werden, bevor sie nützlich verwendet werden können. Mit neuester Technologie können wir einen guten Job bei der Erstellung von Datenmodellen machen und wir sehen auch Fortschritte bei der Arbeit mit kleineren Datenmengen. Dennoch ist eine hohe Datenqualität der wichtigste Teil erfolgreicher AI-Anwendungen.

Siehst du AI & ML als Störfaktoren der Schweizer Industrielandschaft? Was sind aus deiner Sicht die grössten anstehenden Veränderungen?
AI ist kein Störfaktor, sondern ein wesentliches Element, die Wettbewerbsfähigkeit auch in Zukunft aufrecht zu erhalten. Mit AI wird die Schweizer Industrie in der Lage sein, sich wiederholende Prozesse und Aufgaben zu automatisieren und qualifiziertes Personal für komplexere und kreativere Arbeiten einzusetzen. Gleichzeitig wird AI die Menschen dabei unterstützen, schnellere und bessere Entscheidungen zu treffen, zum Beispiel bei der Echtzeit-Analyse von Daten.

Wie können AI, ML und Deep Learning deiner Einschätzung nach zur Entwicklung der Cyber Security beitragen?
Neueste AI-Technologie kann verwendet werden, um grosse Datenmengen zu analysieren und Anomalien leicht zu finden. Auf diese Weise können Sicherheitsvorfälle früher oder noch bevor sie zu einem ernsten Problem werden, erkannt werden. Die AI-Technologie ersetzt nicht bestehende Systeme oder Experten, sondern reduziert den häufig manuellen Aufwand, vermindert die Reaktionszeit und erhöht damit die Gesamtsicherheit eines Unternehmens.

An welchem Projekt arbeitest du aktuell?
Wir entwickeln ein neue Plattform für den Dialog zwischen unseren Kunden und uns. Swisscom wickelt jährlich rund 20 Millionen Kundeninteraktionen ab. Die Zahl steigt kontinuierlich an, da viele Kunden in der Regel mehrere Kanäle nahtlos nutzen. Ein qualitativ hochwertiger Service auf allen Kanälen ist daher für ein exzellentes Kundenerlebnis unerlässlich. Der Kunde soll nicht bei einem Wechsel von einem Kanal zum nächsten seine Angaben erneut machen müssen. Deshalb baut Swisscom

eine neue, AI-basierte Dialogplattform auf, um die verschiedenen Interaktionskanäle aufeinander abzustimmen und den Kunden bestmöglich zu unterstützen.

3.2 Anwendungen von AI & ML in der Cyber Security

Wie wir mit dem Lagebild 2018 aufgezeigt haben, führen aktuell mehrere Trends dazu, AI & ML-Lösungen für Cyber-Security-Massnahmen zu entwickeln und einzusetzen.

- Immer grössere Datenmengen und AI & ML-Anwendungen auszuwerten könnte missbräuchlich ausgenutzt werden, um zum Beispiel gezielte Angriffe effizienter durchzuführen.
- Die Verlagerung immer grösserer Werte in den virtuellen Raum erhöht dadurch auch die Motivation organisierter Krimineller, neue Technologien einzusetzen, um diese Werte zu stehlen oder zu kompromittieren.
- Der anhaltend schnell steigende Bedarf an Cyber-Security-Experten führt bereits heute zu Schwierigkeiten, ausreichend viele Top-Talente auszubilden, in die Unternehmen zu bringen, zu entwickeln und zu halten. Die Situation wird sich in den kommenden Jahren noch deutlich verschärfen.

3.2.1 Security Operation Center

Eine Säule einer ausgereiften Cyber-Sicherheitsstrategie ist die Fähigkeit, zu erkennen, dass ein Angriff stattgefunden hat. Diese Aufgabe wird durch das Security Operation Center (SOC) erfüllt.

Eine wichtige Aufgabe eines SOC-Analysten ist es dabei, relevante von nicht relevanten (sogenannte false positives) Ereignissen zu unterscheiden und nur die relevanten (true positives) als Vorfall bzw. als Sicherheits-Vorfall weiter zu bearbeiten. Die Analysten erfüllen diese Aufgaben bereits heute mit z. B. regel-basierten Werkzeugen. Diese sind jedoch nur so gut, wie die vorher definierten Regeln. Ihre Schwäche ist daher, dass sie nicht schnell auf Änderungen und aussergewöhnliche, nicht vorhergesehene Vorfälle reagieren können. Mit steigenden Datenmengen und intelligenteren Angriffen werden regelbasierte Werkzeuge nicht mehr ausreichen, um Unternehmen und deren Kunden vor Angriffen zu schützen.

Intelligente und selbst lernende Systeme sind der Schlüssel, um die Fähigkeit, Angriffe zu verhindern oder zumindest frühzeitig zu erkennen und abwehren zu können, weiterzuentwickeln. Darüber hinaus können diese Systeme nicht nur selbstständig Bedrohungen erkennen, sondern auch aktiv nach Schwachstellen in einer Systemkonfiguration suchen und Korrekturmassnahmen vorschlagen oder direkt umsetzen.

3.2.2 Phisherman

Bei Swisscom setzen wir bereits auf maschinelles Lernen, um Sicherheitsbedrohungen anzugehen. Phishing ist eine Bedrohung, die unser Geschäft und unsere Kunden täglich betrifft. Beim Phishing versuchen Kriminelle zum Beispiel, durch gefälschte E-Mails an Benutzerdaten wie Passwörter oder Kreditkartendaten zu gelangen.
Der Eckpfeiler der Phishing-Prävention ist es, betrügerische E-Mails korrekt und schnell zu erkennen und von echten zu unterscheiden. Phishing-Angriffe werden immer gezielter und professioneller, so dass selbst sorgfältige und technisch versierte Anwender nicht immer in der Lage sind, Phishing-Angriffe eindeutig als solche zu erkennen.
Hier bringt maschinelles Lernen seinen Mehrwert. Phisherman, unsere Anwendung zur Verhinderung von Phishing-Angriffen, nutzt fortgeschrittene Techniken des maschinellen Lernens, um Phishing-Versuche zu erkennen und zu qualifizieren.

Die folgende Abbildung ist ein aktueller Auszug aus Phisherman mit einem Trendvergleich von 2016 und 2017.
«Top phished Unternehmen» bedeutet, dass Angreifer versucht haben, sich anderen Personen gegenüber als das genannte Unternehmen auszugeben. Am häufigsten wird das durch gefälsche E-Mails versucht. Deutlich ist erkennbar, dass 2016 vor allem US-amerikanische Unternehmen und deren Kunden betroffen waren, während 2017 vermehrt Schweizer Unternehmen betroffen waren. Während der «Spitzenplatz» unverändert bei Apple bleibt und Swisscom in beiden Jahren an fünfter Stelle steht, sind in 2017 neu die UBS und Postfinance stark betroffen.

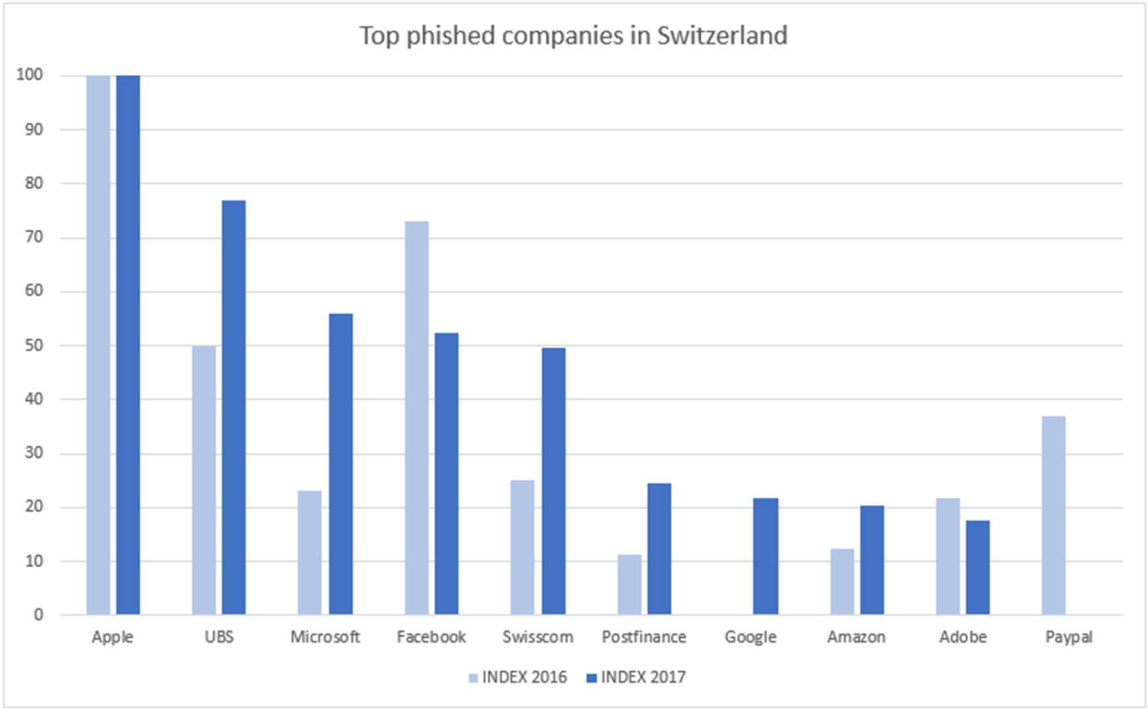


Abbildung 3: Top phished Unternehmen in der Schweiz, Auswertung 2016/17 durch Swisscom Phisherman

Aus dieser Veränderung lässt sich die Aussage ableiten, dass Phishing-Angriffe gezielter, intelligenter und damit unter anderem auch regionaler geworden sind. Je näher die Angreifer am realen Lebensumfeld der betroffenen Personen sind, desto leichter fällt es ihnen, sie zu täuschen und Nutzen daraus zu ziehen.

3.3 Fazit

Der Einsatz von AI-Applikationen wird kurz- bis mittelfristig ein entscheidender Faktor in der Cyber Security sein. Wie aufgezeigt, sind die stetig wachsenden Datenmengen durch bestehende und unterstützende Systeme nicht mehr sinnvoll für Security-Analysten auswertbar. Weiter werden die Angriffe immer intelligenter und gezielter. Auch wenn AI-Applikationen benötigt werden, um kritische von unkritischen Ereignissen zu unterscheiden, sollten diese Systeme vorerst nur unterstützend eingesetzt werden. Die Entscheidungsverantwortung muss so lange noch bei Spezialisten bleiben, bis sich AI im Alltag über längere Zeit bewährt hat.

4. Bedrohungen im Swisscom Netz

Mit mehreren Millionen Internetzugängen und als Anbieter von IT- und Telekommunikations-Infrastrukturen für Grossunternehmen ist Swisscom täglich und in grossem Mass von unterschiedlichsten Bedrohungen betroffen. Diese zielen entweder auf den Endkunden ab oder aber auch auf Swisscom eigene Infrastrukturen.

Um ein Lagebild dieser Bedrohungen erstellen zu können, haben wir über einen Zeitraum von sechs Monaten Daten aus DNS Sinkholes (s. Glossar) und Passive DNS-Daten ausgewertet. Die Analyse zur Erkennung betrachtete primär die DNS-Zugriffe für die Attribution der Bedrohungen innerhalb des Swisscom-Netzes für das Endkunden-Segment. Eine Einschränkung der Aussagekraft dieser Analysemethode besteht darin, dass die Erkennung davon abhängig ist, ob die Domain bekannt ist und in den Sinkhole-Daten erfasst wurde.

Die hier vorgestellten Resultate sollen einen Überblick über die wichtigsten Erkenntnisse geben:

Die Auswertung der erkannten Bedrohungen zeigt eine klare Dominanz von Malware Call Home Traffic (Command and Control), während DNS-Amplifikation und Adware eher ein geringeres Aufkommen haben. Eine weitere sich abbildende Dominanz ist die Kommunikation mit Crypto-Mining-Infrastrukturen.

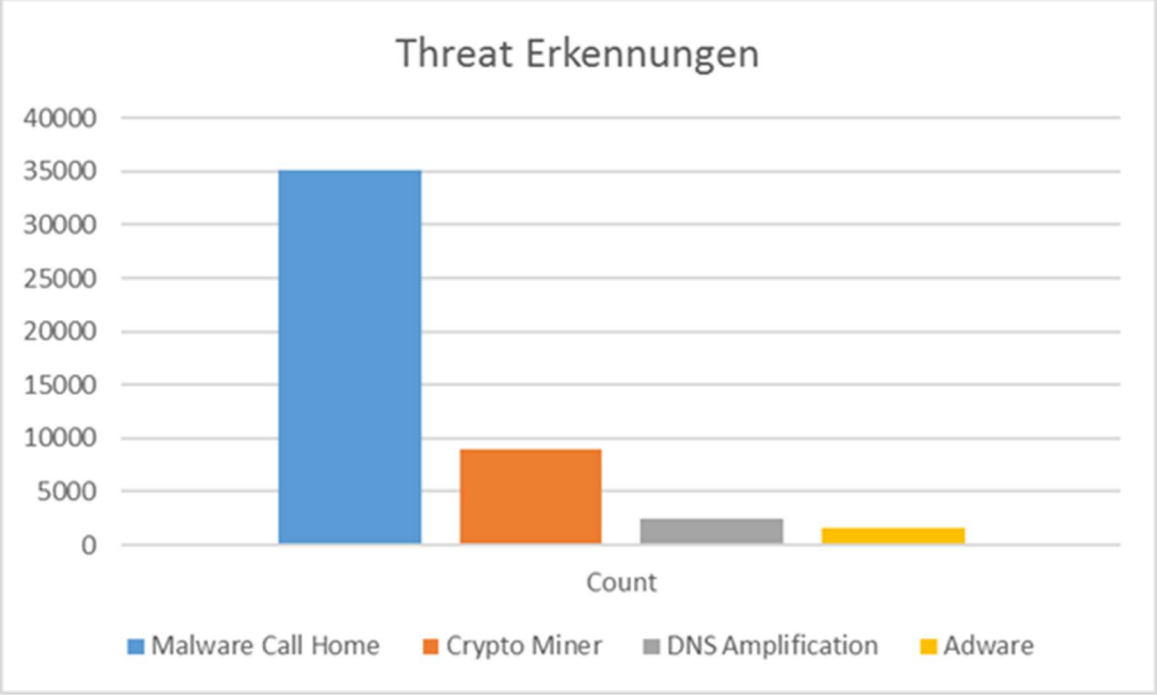


Abbildung 4: Threat Erkennungen

4.1 Malware Call Home

Als Malware Call Home bezeichnen wir typischen Command and Control (CnC) Netzwerkverkehr. Command and Control bezeichnet die Kommunikation eines infizierten Systems (z.B. ein Bot) mit dem unter der Kontrolle eines Angreifers stehenden Systems. Um weiterhin die Kontrolle über das befallene System behalten zu können und Aktionen wie DDoS-Angriffe, das Versenden von Spam E-Mails oder das Infizieren weiterer Systeme durchführen zu können, benötigt der Angreifer diesen Kanal. Innerhalb des Endkunden-Netzes von Swisscom sind insbesondere Conficker, Ramnit und Gamut vertreten. Da bei Ransomware oft keine Command and Control Komponente verwendet wird, ist die Erkennung von Ransomware über DNS-Anfragen nur schwer möglich. Eine Ausnahme stellt die Ransomware WannaCry dar, die über die Kill-Switch Domain erkannt werden kann.

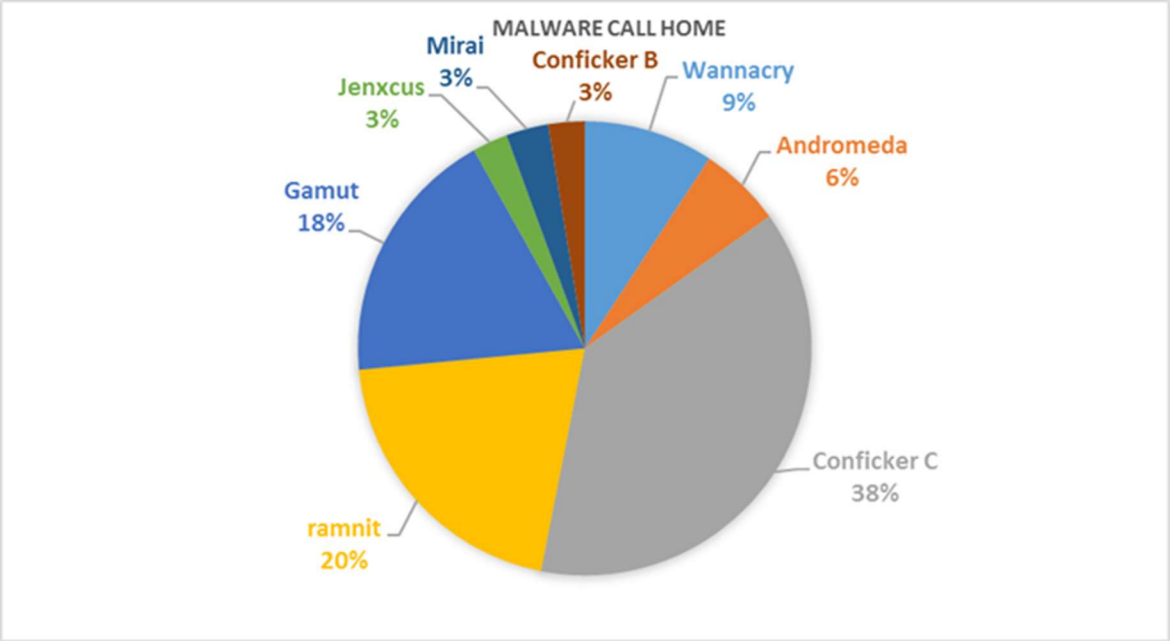


Abbildung 5: Malware Call Home

Die Resultate repräsentieren erkannte Zugriffe auf bereits geblockte Infrastrukturen über die DNS Sinkholes.

Conficker, auch als Downadup bekannt, ist seit dem Jahr 2008 in unterschiedlichen Varianten aufgetaucht und hat Millionen von Windows-Systemen infiziert. Die Malware nutzte eine Schwachstelle im Server Service von Microsoft Windows aus und verwendete in den Versionen B und C eine Dictionary Attack und das Ausnutzen von Windows Autorun, um sich selbst zu propagieren. Die Version C ist die in der Schweiz am häufigsten vorkommende Malware-Familie. Eine Working Group (Conficker Working Group) wurde explizit gegründet, um Conficker zu stoppen. Die Working Group konnte die weitere Verbreitung von Conficker aufhalten. Wer die Akteure hinter Conficker waren, ist bis heute unklar.

Ramnit ist ein modular aufgebautes Malware Toolkit und geniesst bereits seit 2010 unter Cyber-Kriminellen hohe Popularität. Die Malware ist in der Lage, das Web-Browsing-Verhalten der Opfersysteme mitzuverfolgen und z. B. eingegebene Zugangsdaten mitzulesen und zu exfiltrieren. Das Toolkit nutzt mehrere Methoden, um auf einem infizierten System persistent zu bleiben. Unter anderem werden .exe, .dll, .htm und .html Dateien infiziert. Die Malware kopiert sich selbst auf alle verbundenen Festplatten (auch Geräte, die über USB verbunden sind) und werden infiziert. Ramnit Infektionen sind in der Schweiz weiterhin sehr stark vertreten.

Gamut ist ein Spamming Botnet, das Windows Systeme hijacked, um Spam zu versenden. Laut einer aktuellen Analyse war Gamut gemeinsam mit dem Spam Botnetz Necurs für 97% aller Spam E-Mails im letzten Quartal von 2017 verantwortlich.

4.1.1 WannaCry

Obwohl ein geringeres Aufkommen bei WannaCry in unserem Netz zu verzeichnen ist, wollen wir aufgrund der besonderen Eigenschaften dieser Ransomware dennoch darauf eingehen. Bisher bekannte Ransomware zeichnete sich dadurch aus, dass sie durch Spam E-Mails, infizierte Webseiten oder über Botnetze auf ihre Zielsysteme gelangte und dort verblieb, um von ihren Opfern Geld zu erpressen. Ransomware geniesst insbesondere bei Cyber-Kriminellen hohe Popularität. Die unserer Ansicht nach wichtigsten Gründe dafür sind in der folgenden Tabelle aufgeführt.

Low Entry Barrier	Eine zunehmende Professionalisierung von Ransomware as a Service Angeboten ermöglicht auch Kriminellen ohne Programmierkenntnisse oder technischem Know-how, Ransomware-Angriffe durchführen zu können.
Anonymer Geld-transfer	Durch die Verbreitung von anonymen Cryptowährungen wie Monero können Cyber-Kriminelle weltweit agieren und global digitales Geld von ihren Opfern erpressen, ohne erkannt zu werden und nachvollziehbar zu sein.
Hilflosigkeit der Opfer	Besonders Privatanwender und KMUs, die keine Backupstrategie für ihre Daten haben, sehen die Zahlung des Erpressergeldes als einzige Möglichkeit, ihre Daten wieder zu erhalten.

Mit WannaCry wurde erstmalig eine neue Dimension der automatisierten Ransomware-Infektion erreicht. Die im Mai 2017 erkannte WannaCry-Kampagne nutzte den vorher bekannt gewordenen ETERNALBLUE Exploit aus, aus dem ungewollt veröffentlichten NSA-Arsenal. Innerhalb weniger Tage wurden mehr als 230'000 Systeme in mehr als 150 Ländern automatisiert infiziert. Unter den

Betroffenen waren auch kritische Infrastrukturen wie der National Health Service oder die Deutsche Bahn[2].

Abbildung 6: WannaCry Infektion

Die Schweiz war und ist von der WannaCry-Kampagne ebenfalls betroffen, kritische Infrastrukturen waren aber anders als in vielen anderen Ländern nicht betroffen. Global betrachtet zeigt der Angriff jedoch beispielhaft, dass über die Ausnutzung einer einzelnen Schwachstelle über laterale Propagierungsmechanismen eine Pandemie entstehen kann und Netzwerkgrenzen – wie den Perimeter und das interne Netzwerk – verschmelzen lassen und die Verletzbarkeit unserer vernetzten Systeme und unseres digitalen Zeitalters offen legen.

[2] https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html

4.2 Crypto Mining

Während Crypto-Währungen sich weiterhin grosser Beliebtheit bei Ransomware Angriffen erfreut, hat sich ein weiterer, neuer Trend in den erkannten Bedrohungen im Netzwerk von Swisscom gezeigt: Das Minen[3] von Crypto-Währungen. Unter dem Minen von Crypto-Währungen verstehen wir das unerlaubte Minen von Crypto-Währungen z.B. durch die unerlaubte Installation von Minern durch:

Insider	Die kostenlose Mining-Möglichkeit mit den Ressourcen (Rechenpower) und auf Kosten des Unternehmens (Strom) macht Mining attraktiv für Mitarbeitende von Unternehmen. Mitarbeitende mit besonderen Privilegien (z. B. Administratoren, Power-User) könnten diese ausnutzen[4].
Malware	Im Gegensatz zu Ransomware mit einmaligen Zahlungen gewährleisten Miner regelmässige Einnahmen und sind somit deutlich lukrativer für Cyber Kriminelle.
Drive By Mining	Drive By Mining wird direkt über Skriptsprachen im Browser durchgeführt und nutzt die CPU Leistung der Webseiten Besucher.

Eine generelle Auswertung unserer passiven DNS-Daten zeigt, welche Pools aktiv für das Minen von Cryptowährungen genutzt werden.

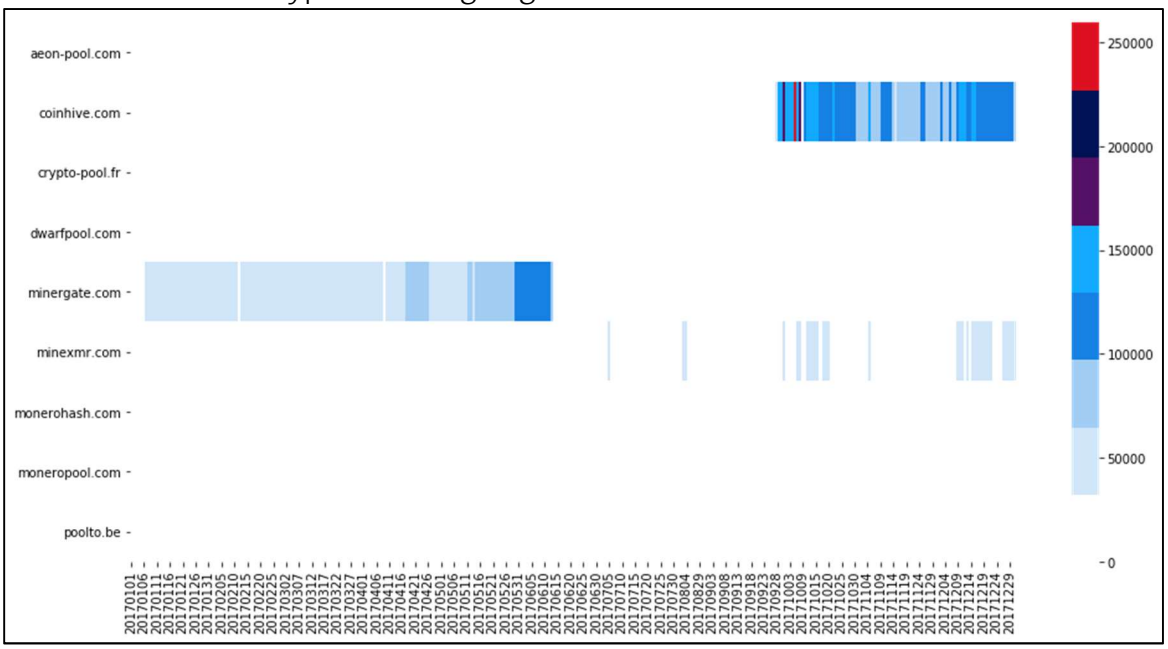


Abbildung 7: Mining Pool Nutzung

[3] Beim Minen (deutsch: Schürfen) wird Rechenleistung verwendet, um Transaktionen von Cryptowährungen zu bestätigen. Miner werden finanziell incentiviert.
[4] https://www.rferl.org/a/russia-sarov-nuclear-facility-workers-arrested-using-supercomputer-mine-bitcoin/29030004.html

Die weissen Einträge befinden sich unterhalb von 50'000 Aufrufen pro Tag. Besonders hervorzuheben sind die Pools minergate.com sowie coinhive.com. Die Nutzung dieser Pools lässt generell nicht auf eine bosärtige Absicht schliessen, Cyber-Kriminelle haben jedoch längst damit begonnen, ihre Schadsoftware mit einem Cryptominer auszustatten und greifen bei diesem lukrativen Modell zur Monetarisierung infizierter Rechner auf die bewährten Mining Pools zurück.

Die Profileration von Miner-Installationen betrifft Clients, Server und auch Browser.

4.2.1 Coinhive

Insbesondere Coinhive erfreut sich grosser Beliebtheit bei Angreifern um Crypto-Währungen via Drive By Mining zu minen. Da Coinhive direkt im Browser eines Opfers ausgeführt wird und via Javascript die CPU-Leistung von Webseitenbesuchern nutzt, um die Crypto-Währung Monero zu minen, lässt es sich einfach nutzen und hat keine Betriebskosten für die Cyber-Kriminellen. Um die grösstmöglichen Ausschüttungen zu erhalten, zielen Cyber-Kriminelle auf hoch frequentierte Webseiten. Längst sind somit bereits auch schon Regierungswebseiten zum Ziel geworden, auf denen das Coinhive Mining Javascript integriert wurde und zu Drive-By Mining-Angriffen missbraucht wurde[5].

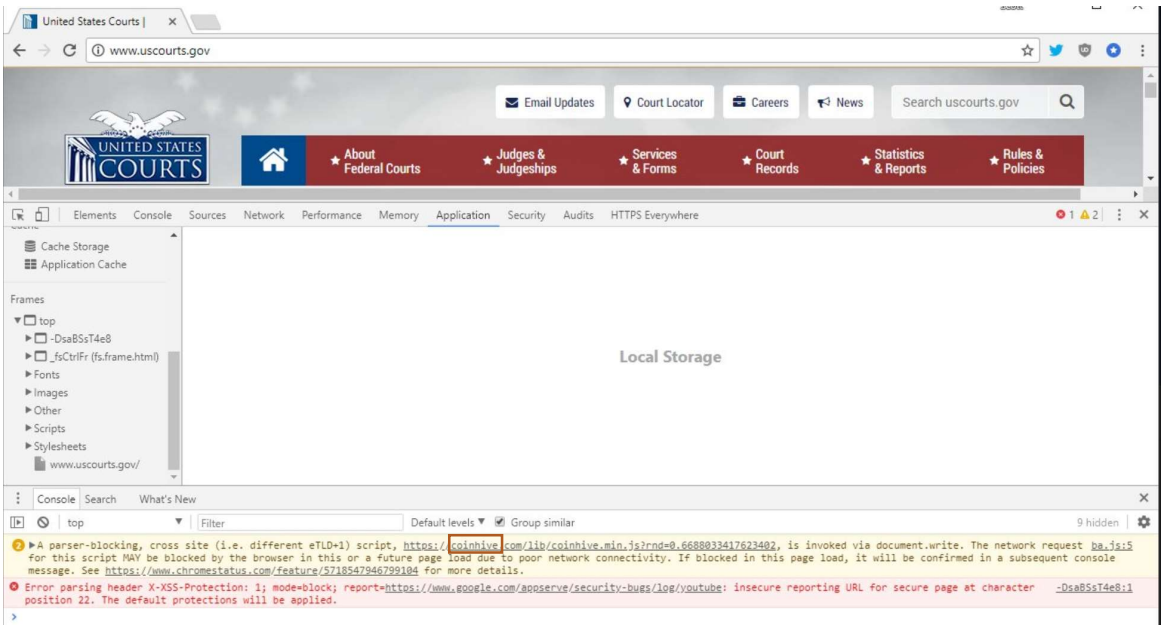


Abbildung 8: Webseite des United States Courts mit dem Coinhive Javascript Infiziert.

In einer aktuellen Analyse nutzten wir die Webseite publicwww.com, um Webseiten zu identifizieren, die das Coinhive Javascript laden.

[5] https://twitter.com/Scott_Helme/status/962684239975272450

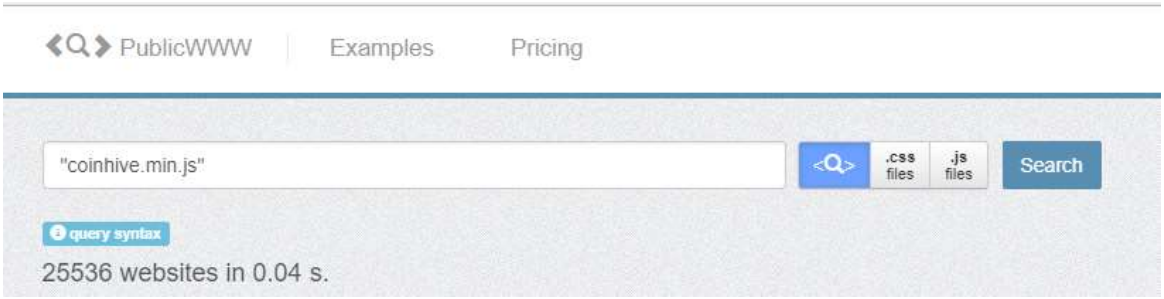


Abbildung 9: Coinhive auf publicwww

Insgesamt wurden mehr als 25'500 Webseiten identifiziert, die über Coinhive Drive-By-Mining-Operationen auf den Endgeräten von Webseitenbesuchern durchführen. Viele dieser Webseiten wurden als kompromittiert identifiziert[6].

4.3 Fazit

Mit Conficker, Gamut, Ramnit und WannaCry Infektionen sind Malware-Familien mit unterschiedlichem Verwendungszweck bei Endkunden innerhalb des Swisscom Netzes vertreten. Die Infektionen von Conficker deuten darauf hin, dass viele der infizierten Systeme noch Legacy Betriebssysteme verwenden, die für die von Conficker ausgenutzte Schwachstelle noch anfällig sind. Die Gamut- und Ramnit-Infektionen zeigen, dass Cyber-Kriminelle eine hohe Anzahl an schweizerischen Endkundensystemen unter ihre Kontrolle gebracht haben und diese für Ihre Zwecke missbrauchen. Auch wenn die Schweiz wenig von WannaCry betroffen war, müssen wir in der Folge davon ausgehen, dass durch die zunehmende Digitalization (s. Threat Radar) die Gefahr einer weiteren «ausser Kontrolle» geratenen Cyberwaffe mit globalen Auswirkungen steigt.

Die Auswertung der Mining Pools für Crypto-Währungen hat eine hohe Anzahl von möglichen drive-by-cryptomining-Zugriffen gezeigt. Das lukrative Modell und die Anonymität bei Crypto-Währungen macht diese neue Technologie insbesondere für Cyber-Kriminelle interessant. Neben der Installation von Minern durch Insider oder drive-by-Mining wie Coinhive könnten auch Unternehmen dazu übergehen, die vorhandenen Unternehmensressourcen zu nutzen, um Mining zu betreiben.

Als Internet Service Provider gewährleistet Swisscom einen reibungslosen barrierefreien und sicheren Internet-Zugang für unsere Kunden und unsere Gesellschaft. Wir sind einerseits verpflichtet, unsere Kunden zu schützen, andererseits dürfen wir die Offenheit des Netzes nicht beeinträchtigen und stehen für ein offenes Internet in der Schweiz ein[7].

[6] https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/
[7] https://asut.ch/asut/media/id/153/type/document/bv_verhaltenskodex_mit_asut_201603.pdf

Um den Schutz vor Malware sicherzustellen, haben wir bereits unterschiedliche etablierte Mechanismen im Einsatz, wie:

Spam Traps	Spam Traps sind E-Mail-Adressen ohne Benutzer, welche zum Zweck erstellt wurden, illegitime E-Mails wie Spam, Phishing oder Malware-Attacken zu erkennen. Swisscom betreibt tausende solcher Mailkonten, deren Inhalt automatisiert analysiert wird und in die Schutzfilter einfliesst.
Internet Guard	Der Swisscom Internet Guard funktioniert auf Basis von Blacklists von Drittanbietern und eigenen Blacklists, die auf unseren DNS Servern eingespiesen und blockiert werden. Durch die Nutzung der Internet Guard-DNS-Infrastruktur sind Swisscom Kunden von als bösartig erkannten Webseiten geschützt.
Kundenmeldungen	Betrügerische Webseiten (z.B. Phishing oder Betrugsversuch), Webseiten mit einer Schadsoftware (Virus, Trojaner, etc.) und solche, die eine Sicherheitslücke auf Geräten ausnützen, können direkt per E-Mail an spamreport@bluewin.ch gemeldet werden.

Kunden, die bereits mit Malware infiziert sind, werden in einer Sandbox – einem isolierten Quarantänenetzwerk — terminiert. Dem Kunden wird bei einem Verbindungsversuch eine Informationsseite angezeigt, welche über die Massnahme sowie deren Grund informiert und weitere Information mit Hilfe zur Selbsthilfe anbietet. Nicht betroffen von der Sperre sind Swisscom TV sowie die Telefonie. Weiterhin möglich sind auch Verbindungen, welche dem Kunden helfen, das Problem zu beheben, z. B. durch Antivirenprogramme, Software Updates etc.

5. Glossar

0-Day/Zero-Day Exploit	Software-Exploit, der vor oder mit der ersten Veröffentlichung einer Sicherheitslücke bekannt ist. D.h., der Exploit ist verfügbar, bevor der Softwarehersteller einen Sicherheitspatch bereit hat.
API	Application Programming Interface Schnittstelle, die es Programmen erlaubt, mit einer gemeinsamen Sprache direkt Daten auszutauschen (Maschine zu Maschine).
Backdoor	Software-Hintertüre, um unter Umgehung des Zugriffsschutzes auf einen Computer zuzugreifen.
Botnet	Netzwerk einer grossen Anzahl kompromittierter Computer, welche zentral durch einen Botmaster kontrolliert werden.
Defacement	Einbringen von unerwünschten Inhalten in eine gehackte Website.
DoS, DDoS	Denial of Service (DoS) Ein System wird durch eine grosse Anzahl an Anfragen lahmgelegt. Distributed Denial of Service (DDoS) Der DoS Angriff geht gleichzeitig von einer grossen Zahl verteilter Systeme aus (z.B. ein Botnet). Ein einfaches Blockieren des Angreifers ist nicht mehr möglich.
DNS Sinkhole	DNS Sinkholes werden primär vewendet, um eine als bösartig erkannte Domain via DNS auf eine andere IP-Addresse zu leiten.
Exploit	Programm, Code oder Befehlsfolgen, mit denen sich Schwachstellen in einer Software ausnutzen lassen.
Exploit Mitigation	Allgemeiner Begriff für Techniken, welche das Ausnutzen von Schwachstellen auf Systemen unterbinden oder erschweren.
ICS	Industry Control System Allgemeine Bezeichnung für Industriekontrollsysteme, siehe SCADA.
ICT	Information and Communication Technology Abkürzung für die Informatik- und Telekommunikationsindustrie.
Jamming	Absichtliches Stören von Funkkommunikation.
Kill-Switch	Versteckte Software, die auch auf Befehl von aussen reagieren kann, die Funktionsweise eines Systems stört oder das System unbrauchbar macht.
Malware	Software, welche schädliche und nicht gewollte Funktionen ausführt.

Money Mule	Kriminelle verleiten Personen dazu, Geld von „Kunden“ entgegenzunehmen und nach Abzug einer Kommission mit einem Geldüberweisungsdienst weiterzuleiten. Die Person (money mule) glaubt für eine legitime Organisation zu arbeiten.
Monero	Die Kryptowährung Monero hat für Cyber-Kriminelle besondere Vorteile, wie die nicht verfolgbaren Transaktionen und der CryptoNight-Algorithmus, der CPUs und GPUs von Computern und Servern präferiert. Mit dem letztgenannten unterscheidet sich Monero deutlich von Bitcoin im Bezug auf das Mining, wofür mittlerweile spezielle und teure Hardware benötigt wird.
OSINT	Open Source Intelligence Beschaffung von Informationen unter ausschliesslicher Verwendung von öffentlich zugänglichen Quellen.
Patch Sicherheits-Update	Programmcode, der fehlerhafte Software ersetzt, um Sicherheitslücken zu eliminieren.
Phishing	Mit Phishing werden Benutzer durch Tricks (meistens E-Mails mit gefälschten Aufforderungen etwas zu tun) dazu verleitet, sensible Daten preiszugeben.
SCADA	Supervisory Control And Data Acquisition System Systeme zur Überwachung und Steuerung von technischen Prozessen (z.B. Industrieprozessen).
Schwachstelle	Eine Schwachstelle oder Verwundbarkeit in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
SDR	Software Defined Radio. Universelle Hochfrequenzsender und Empfänger, welche die Signalverarbeitung durch Software realisieren und daher durch den Benutzer auf verschiedene Protokolle und Anwendungen adaptierbar sind.
SmartGrid	Intelligentes Stromnetz. SmartGrid umfasst die Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Energieübertragungs- und Verteilungsnetzen.
SmartHome	Intelligentes Heim. Überbegriff für die vernetzte und teilautomatisierte Steuerung von Energie, Unterhaltung und Sicherheit in Wohnungen und Häusern.
Social Media	Webseiten, auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen (z.B. Facebook, Twitter, LinkedIn, Xing).
Spearphishing	Gezielte und personalisierte Phishing-Attacke, z. B. um die Zugangsdaten von Schlüsselpersonen zu bekommen.

Spoofing	Täuschungsversuche in Netzwerken zur Verschleierung der eigenen Identität.