Niedersachsen

Staatsanwaltschaft Verden
Die Leitende Oberstaatsanwältin
– Pressestelle –

ZENTRALE KRIMINALINSPEKTION
LÜNEBURG

POLIZEIDIREKTION
LÜNEBURG

Bundesamt
für Sicherheit in der
Informationstechnik

HANDOUT

zur Pressekonferenz der Staatsanwaltschaft Verden und der Zentralen Kriminalinspektion Lüneburg

01.12.2016
16:00 Uhr

Behördenzentrum Auf der Hude
21339 Lüneburg
Saal 1

Zentrale Kriminalinspektion
LÜNEBURG

Staatsanwaltschaft
VERDEN

Operation Avalanche

Gemeinsame Pressekonferenz

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Bundesamt für Sicherheit in der Informationstechnik

EUROJUST

Presse

Niedersachsen

Staatsanwaltschaft Verden
Die Leitende Oberstaatsanwältin
– Pressestelle –

ZENTRALE KRIMINALINSPEKTION
LÜNEBURG

01.12.2016

AVALANCHE, eine der weltweit größten Infrastrukturen zum Einsatz von Botnetzen wurde in internationaler Zusammenarbeit aufgedeckt und analysiert.

Polizei und Staatsanwaltschaft zerschlagen Strukturen für massenhafte Angriffe auf Online-Banking-Kunden und verhaften maßgebliche Führungsmitglieder einer kriminellen Vereinigung

(gemeinsame Presseinformation der Zentralen Kriminalinspektion Lüneburg und der Staatsanwaltschaft Verden)

Verden (Aller), Lüneburg. Am gestrigen Tage konnten in einer international koordinierten Aktion mutmaßliche Führungsmitglieder einer kriminellen Vereinigung verhaftet werden. Durch die gleichzeitig erfolgte Beschlagnahme von 39 Servern und mehreren hunderttausend Domains wurde den Tatverdächtigen allein in Deutschland die Kontrolle über mehr als 50.000 Opfer-Computer entzogen.

Nach über vier Jahren intensiver Ermittlungsarbeit der Cybercrime-Spezialisten der Zentralen Kriminalinspektion Lüneburg und der Staatsanwaltschaft Verden und in Zusammenarbeit mit dem amerikanischen FBI, dem United States Attorney's Office for the Western District of Pennsylvania, dem Department of Justice sowie den Sicherheitsbehörden von 39 europäischen und außereuropäischen Staaten war es möglich geworden, die wohl weltweit größte Infrastruktur zum Betrieb von Botnetzen aufzudecken und zu analysieren. Bis zum gegenwärtigen Zeitpunkt konnten allein auf der Führungsebene 16 Beschuldigte identifiziert werden. Gegen 7 Tatverdächtige hat das Amtsgericht Verden Haftbefehle wegen Bildung einer kriminellen Vereinigung, banden- und gewerbsmäßigen Computerbetruges und anderer Straftaten erlassen.

Mit der strukturierten Zusammenlegung von mehreren Botnetzen war es den Tätern gelungen, Bankkunden, die ihre Geschäfte online erledigten, um durchschnittlich mehr als 5.000 EUR zu schädigen. Mindestens seit 2009 nutzten die Täter die weltweit vernetzte Botnetz-Infrastruktur „AVALANCHE“ für Phishing- und Spamkampagnen. Pro Woche wurden mehr als eine Million Spammails mit schädigendem Anhang oder Link versandt. Durch Öffnen des Anhangs oder Anklicken des Links wurde das nunmehr infizierte Computer-System Teil des Botnetzes. Auf diese Weise wurden durch die Täter zeitgleich mehr als 50.000 Opfer-PCs kontrolliert und ausspioniert. Aufgrund der hier vorliegenden Anzeigen kann die Schadenssumme derzeit auf ca. 6 MioEUR aus 1.336 Taten beziffert werden. Der

tatsächliche Schaden dürfte auch in Deutschland weitaus höher liegen, während die genannten Zahlen sowieso nur die Angriffe gegen Opfer in Deutschland wiedergeben.

Begonnen hatten die Ermittlungen allerdings vor vier Jahren, als massenhaft sog. Ransomware verbreitet wurde, mit der private und geschäftliche Nutzer von PCs und PC-Netzwerken erpresst wurden, Geld zu zahlen. Während die Ermittler mit der Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) in Bonn hinter die enormen Dimensionen der Botnetzinfrastuktur „AVALANCHE" kamen, wechselten die Tatverdächtigen nicht nur die Geschäftsfelder, sondern auch die Server und die Länder von denen aus sie agierten. Derzeit liegt der Schwerpunkt darin, Online-Banking-Kunden zu schädigen. "Die Tücke einer ausgefeilten Botnetz-Infrastruktur liegt darin, dass allein das Abschalten eines einzelnen Botnetzes nicht ausreicht, um die kriminellen Angriffe zu unterbinden", teilte der Leiter der Zentralstelle für Cybercrime der Staatsanwaltschaft Verden, Oberstaatsanwalt Frank Lange mit. "Die Aufgaben der entdeckten und unschädlich gemachten Server werden schlagartig von den Servern der anderen Botnetze übernommen, bis ein neues weiteres Botnetz aufgebaut wird". Durch die Analyse der Strukturen von AVALANCHE und die Identifizierung der einzelnen Server auf Führungsebene wurde der Grundstein für die gestrige Zerschlagung der Infrastruktur gelegt. Unterstützt durch die europäischen Behörden EUROJUST und EUROPOL erfolgten zeitgleich in 10 Ländern der Welt Durchsuchungen, Beschlagnahmen von Servern und Domains sowie Festnahmen aufgrund bestehender Haftbefehle. Die identifizierten Tatverdächtigen kommen aus 10 verschiedenen Ländern. In einzelnen Fällen wird es nicht möglich sein, die Beschuldigten in Deutschland vor Gericht zu stellen, weil entsprechende Auslieferungsabkommen fehlen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilt dazu folgendes mit:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt nach einem Amtshilfeersuchen die ZKI Lüneburg sowie die StA Verden bei der Analyse der Botnetzinfrastruktur AVALANCHE und der verwendeten Schadsoftware. Das Nationale Cyber-Abwehrzentrum koordiniert aktuell BSI-seitig die Zerschlagung der Botnetzinfrastruktur. Die Analysen haben ergeben, dass rund 20 verschiedene Botnetze diese Infrastruktur nutzen, um u.a. Spam- und Phishing-E-Mails zu versenden, Ransomware zu verbreiten und die Nutzer von Online-Banking-Angeboten zu betrügen.

Im Rahmen der Zerschlagung werden nun sogenannte Sinkhole-Server eingesetzt, mit deren Hilfe betroffene Kunden gewarnt werden können. Dies erfolgt durch die Internetserviceprovider auf Basis der BSI-Analyse. Bereits im laufenden Ermittlungsverfahren wurde zur Warnung der Nutzer das Providerinformationssystem (PI) aufgebaut. Hierbei werden durch das BSI Mitteilungen über infizierte Systeme an die Provider übermittelt. Seit 2014 wurden so bereits mehr als 4,5 Millionen Meldungen an die deutschen Provider und über diese an die Kunden gesendet.

Die Zerschlagung der Botnetzinfrastruktur ist allerdings nur ein erster Schritt. Die Schadprogramme auf den infizierten Rechnern werden dadurch nicht gelöscht. Dies muss durch die Nutzer selbst erfolgen. Die betroffenen Bürgerinnen und Bürger werden über ihre Provider informiert. Ihnen wird dringend empfohlen, ihre Rechner auf eine Infektion mit

Schadprogrammen zu überprüfen. Nähere Informationen dazu erhalten Sie unter www.bsi-fuer-buerger.de/botnetz.

Einladung zur Pressekonferenz:

Für weitere Informationen laden die Zentrale Kriminalinspektion der Polizeidirektion Lüneburg und die Staatsanwaltschaft Verden die Medienvertreter

am 01.12.2016, 16:00 Uhr MEZ

in Lüneburg

zu einer Pressekonferenz ein.

Anschrift:
Polizeidirektion Lüneburg,
Behördenzentrum Auf der Hude,
Auf der Hude 2,
21339 Lüneburg.

Teilnehmer der Pressekonferenz werden Vertreter von Polizei und Justiz und der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) sein.

Kontakt:

Lutz Gaebel
Pressesprecher
Staatsanwaltschaft Verden
Die Leitende Oberstaatsanwältin
- Pressestelle -
Johanniswall 8
27283 Verden (Aller)

Tel: +49-4231-18-436 (am 01.12.2016 nicht erreichbar)
Mobil: +49-151-59087764
Fax: +49-4231-18-887
E-Mail: lutz.gaebel@justiz.niedersachsen.de

Europol - Eurojust joint press release

'Avalanche' network dismantled in international cyber operation

The Hague, 1 December 2016 / 16:00 CET

On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform.

The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. As a result, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. Also, 221 servers were put offline through abuse notifications sent to the hosting providers. The operation marks the largest-ever use of sinkholing* to combat botnet** infrastructures and is unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked.

On the action day, Europol hosted a command post at its headquarters in The Hague. From there, representatives of the involved countries worked together with Europol's European Cybercrime Centre (EC3) and Eurojust officials to ensure the success of such a large-scale operation.

In addition Europol supported the German authorities throughout the entire investigation by assisting with the identification of the suspects and the exchange of information with other law enforcement authorities. Europol's cybercrime experts produced and delivered analytical products.

Eurojust's Seconded National Expert for Cybercrime assisted by clarifying difficult legal issues that arose during the course of the investigation. Several operational and coordination meetings were also held at both Europol and Eurojust.

Julian King, European Commissioner for the Security Union, said: "Avalanche shows that we can only be successful in combating cybercrime when we work closely together, across sectors and across borders. Cybersecurity and law enforcement authorities need to work hand in hand with the private sector to tackle continuously evolving criminal methods. The EU helps by ensuring that the right legal frameworks are in place to enable such cooperation on a daily basis".

Rob Wainwright, Europol Director, said: "Avalanche has been a highly significant operation involving international law enforcement, prosecutors and Industry resources to tackle the global nature of cybercrime. The complex trans-national nature of cyber investigations requires international cooperation between public and private organisations at an unprecedented level to successfully impact on top level cybercriminals. Avalanche has shown that through this cooperation we can collectively make the internet a safer place for our businesses and citizens".

Ms Michèle Coninsx, President of Eurojust, said: 'Today marks a significant moment in the fight against serious organised cybercrime, and exemplifies the practical and strategic importance of Eurojust in fostering international cooperation. Together with the German and US authorities, our EU and international partners, and with support from Eurojust and EC3, Avalanche, one of the world's largest and most malicious botnet infrastructures, has been decisively neutralised in one of the biggest takedowns to date.'

The criminal groups have been using the Avalanche infrastructure since 2009 for conducting malware, phishing and spam activities. They sent more than 1 million e-mails with damaging attachments or links every week to unsuspecting victims.

The investigations commenced in 2012 in Germany, after an encryption ransomware*** (the so-called Windows Encryption Trojan), infected a substantial number of computer systems, blocking users' access. Millions of private and business computer systems were also infected with malware, enabling the criminals operating the network to harvest bank and e-mail passwords.

With this information, the criminals were able to perform bank transfers from the victims' accounts. The proceeds were then redirected to the criminals through a similar double fast flux infrastructure, which was specifically created to secure the proceeds of the criminal activity.

The loss of some of the network's components was avoided with the help of its sophisticated infrastructure, by redistributing the tasks of disrupted components to still-active computer servers. The Avalanche network was estimated to involve as many as 500,000 infected computers worldwide on a daily basis.

What made the 'Avalanche' infrastructure special was the use of the so-called double fast flux technique****. The complex setup of the Avalanche network was popular amongst cybercriminals, because of the double fast flux technique offering enhanced resilience to takedowns and law enforcement action.

Malware campaigns that were distributed through this network include around 20 different malware families such as *goznym, marcher, matsnu, urlzone, xswkit, and pandabanker*. The money mule schemes operating over Avalanche involved highly organised networks of "mules" that purchased goods with stolen funds, enabling cyber-criminals to launder the money they acquired through the malware attacks or other illegal means.

In preparation for this joint action, the German Federal Office for Information Security (BSI) and the Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) analysed over 130 TB of captured data and identified the server structure of the botnet, allowing for the shut-down of thousands of servers and, effectively, the collapse of the entire criminal network.

The successful takedown of this server infrastructure was supported by Interpol, the Shadows Server Foundation, Registrar of Last Resort, ICANN and domain registries involved in the takedown phase. INTERPOL has also facilitated the cooperation with domain registries. Several antivirus partners provided support concerning victim remediation.

Computer users should note that this law enforcement action will NOT clean malware off any infected computers – it will merely deny the Avalanche users' ability to communicate with infected

victim computers. Avalanche victim computers will still be infected, but shielded from criminal control.

Victims of malware operating over the Avalanche network may use the following webpages created for assistance in removing the malware:

- www.bsi-fuer-buerger.de/botnetz and www.bsi-fuer-buerger.de/avalanche, in German;
- www.bsi-fuer-buerger.de/EN/botnetz and www.bsi-fuer-buerger.de/EN/avalanche, in English;
- https://us-cert.gov/avalanche;
- www.nationalcrimeagency.gov.uk/news/962-avalanche-takedown;
- www.getsafeonline.org/news/avalanche;
- www.actionfraud.police.uk/news-police-takedown-computer-network-used-to-infect-millions-of-devices-dec16;
- www.cyberaware.gov.uk/blog.

The Shadowserver Foundation have supported this operation and will be making the sinkhole data available globally to responsible bodies via their free daily remediation feeds (https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork). More information can be found here: http://blog.shadowserver.org/2016/12/01/avalanche/.

Background

* ***Sinkholing*** is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command and control computer systems and so criminals can no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.

** ***Botnets*** are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

*** ***Ransomware*** is a type of malware that infects the victim's PC and encrypts the victim's files, so that the victim is unable to access them. The criminal behind the ransomware then uses intimidation and misinformation to force the victim to pay a sum of money in exchange for the password that unlocks the encrypted files. Even if a password is eventually provided, it does not always work.

**** ***Fast flux technique*** is an evasion technique used by botnet operators to quickly move a fully qualified domain name (a domain that points to one specific Internet resource such as www.domain.com) from one or more computers connected to the Internet to a different set of computers. Its aim is to delay or evade the detection of criminal infrastructure. In the ***double fast flux*** setup, both the domain location and the name server queried for this location are changed.

Figures at a glance

Countries involved: Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.
Number of arrests: 5
Number of searches conducted: 37
Number of servers seized: 39
Number of servers taken offline through abuse notifications: 221

Bundesamt
für Sicherheit in der
Informationstechnik

Pressemitteilung

HAUSANSCHRIFT
Godesberger Allee 185 - 189
53175 Bonn

TEL +49 (0) 22899 9582 - 5777
FAX +49 (0) 22899 9582 - 5400

presse@bsi.bund.de
www.bsi.bund.de

– SPERRFRIST: Donnerstag, 01. Dezember 2016, 16:00 Uhr –

BSI ermöglicht Zerschlagung der Botnetz-Infrastruktur Avalanche

Hilfestellung für Betroffene unter www.bsi-fuer-buerger.de/botnetz

Bonn, 1. Dezember 2016. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt nach einem Amtshilfeersuchen die Zentrale Kriminalinspektion der Polizeidirektion Lüneburg (ZKI) sowie die Staatsanwaltschaft Verden/Aller bei der Analyse und Zerschlagung der Botnetz-Infrastruktur Avalanche. Seitens des BSI hat das Nationale Cyber-Abwehrzentrum die koordinierende Funktion übernommen.

Das BSI als die nationale Cyber-Sicherheitsbehörde hat die technische Grundlage zur Identifizierung der Botnetz-Infrastruktur sowie zur Analyse der von den Cyber-Kriminellen verwendeten Schadsoftware bereitgestellt. Dadurch wurde die Abschaltung der missbrauchten Server und so die Zerschlagung des gesamten kriminellen Netzwerks ermöglicht. Gleichzeitig ermöglicht das BSI die Information der weltweit betroffenen Nutzer, deren Computer und Smartphones von den Tätern mit Schadsoftware infiziert und damit zum Teil der Botnetze gemacht wurden. Die Analysen haben unter anderem ergeben, dass rund 20 verschiedene Botnetze die Avalanche-Infrastruktur nutzen, zum Beispiel um Spam- und Phishing-E-Mails zu versenden, Ransomware zu verbreiten und die Nutzer von Online-Banking-Angeboten zu betrügen.

Hierzu erklärt BSI-Präsident Arne Schönbohm: *„Botnetze sind eine der großen Bedrohungen für die Digitalisierung. Die erfolgreiche Aktion zeigt, dass der Staat handlungsfähig und das Internet kein rechtsfreier Raum ist. Es ist uns gemeinsam gelungen, eine internationale kriminelle Infrastruktur zu zerschlagen und die Bürgerinnen und Bürger vor vielen aktuellen Gefahren im Internet zu schützen.“*

Information der Betroffenen

Im Rahmen der Zerschlagung setzt das BSI zusammen mit Shadowserver, einer Non-Profit-Organisation von IT-Sicherheitsspezialisten, Sinkhole-Server ein, die die von den Kriminellen genutzten und im Rahmen der Strafverfolgungsaktion abgeschalteten

Steuerungsserver der Botnetze ersetzen. Mit Hilfe dieser Sinkhole-Server können betroffene Internetnutzer gewarnt werden. Anhand der IP-Adressbereiche, die verschiedenen Internetserviceprovidern zugeordnet sind, gibt das BSI die einzelnen IP-Adressen gezielt an diese Provider weiter. Nur die Provider können die IP-Adressen einem Netzwerkanschluss zuordnen und so ihre Kunden informieren.

BSI gibt Handlungsempfehlungen

Die Zerschlagung der Botnetz-Infrastruktur führt nicht zu einer automatischen Bereinigung der infizierten Nutzersysteme. Damit die Internetnutzer ihre Computer und Smartphones von der Infektion mit Schadsoftware bereinigen können, gibt das BSI unter www.bsi-fuer-buerger.de/botnetz umfangreiche Hilfestellung.

Pressekonferenz am 1.12.2016 – 16 Uhr

Für weitere Informationen laden die Zentrale Kriminalinspektion der Polizeidirektion Lüneburg und die Staatsanwaltschaft Verden Medienvertreter zu einer Pressekonferenz am 01.12.2016, 16:00 Uhr in die Polizeidirektion Lüneburg ein.

Teilnehmer der Pressekonferenz werden Vertreter von Polizei und Justiz und der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) sein.

Anschrift: Polizeidirektion Lüneburg, Behördenzentrum Auf der Hude, Auf der Hude 2, 21339 Lüneburg.

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: **www.bsi.bund.de**

Operation Avalanche 01.12.2016

Robert Kruse, Polizeipräsident der PD Lüneburg:

„Dieses Verfahren belegt die zunehmende Verlagerung hochgradig krimineller Aktivitäten in den virtuellen Raum. Es ist daher richtig, dass Niedersachsen hier einen strategischen Schwerpunkt gesetzt hat und unter anderem mit der Schaffung von Schwerpunktstaatsanwaltschaften und speziellen polizeilichen Ermittlungseinheiten zur Bekämpfung der Cyberkriminalität dieser Entwicklung Rechnung trägt. Die steigende Bedeutung der internationalen Zusammenarbeit der Sicherheitsbehörden erfordert aber auch eine konsequente Fortentwicklung unserer rechtlichen und taktischen Möglichkeiten, die auf diese neuen Herausforderungen noch besser abgestimmt sein müssen. Ich bedanke mich bei der Staatsanwaltschaft Verden für die äußerst vertrauensvolle Zusammenarbeit und bei allen Beteiligten Behörden des In- und Auslands für die engagierte Kooperation. Mein ganz besonderer Dank gilt meinen eigenen Mitarbeiterinnen und Mitarbeitern für die herausragenden und engagierten Leistungen bei der Bewältigung dieses äußerst komplexen Verfahrens.“

Kriminaldirektor Stefan Mayer, Leiter ZKI Lüneburg:

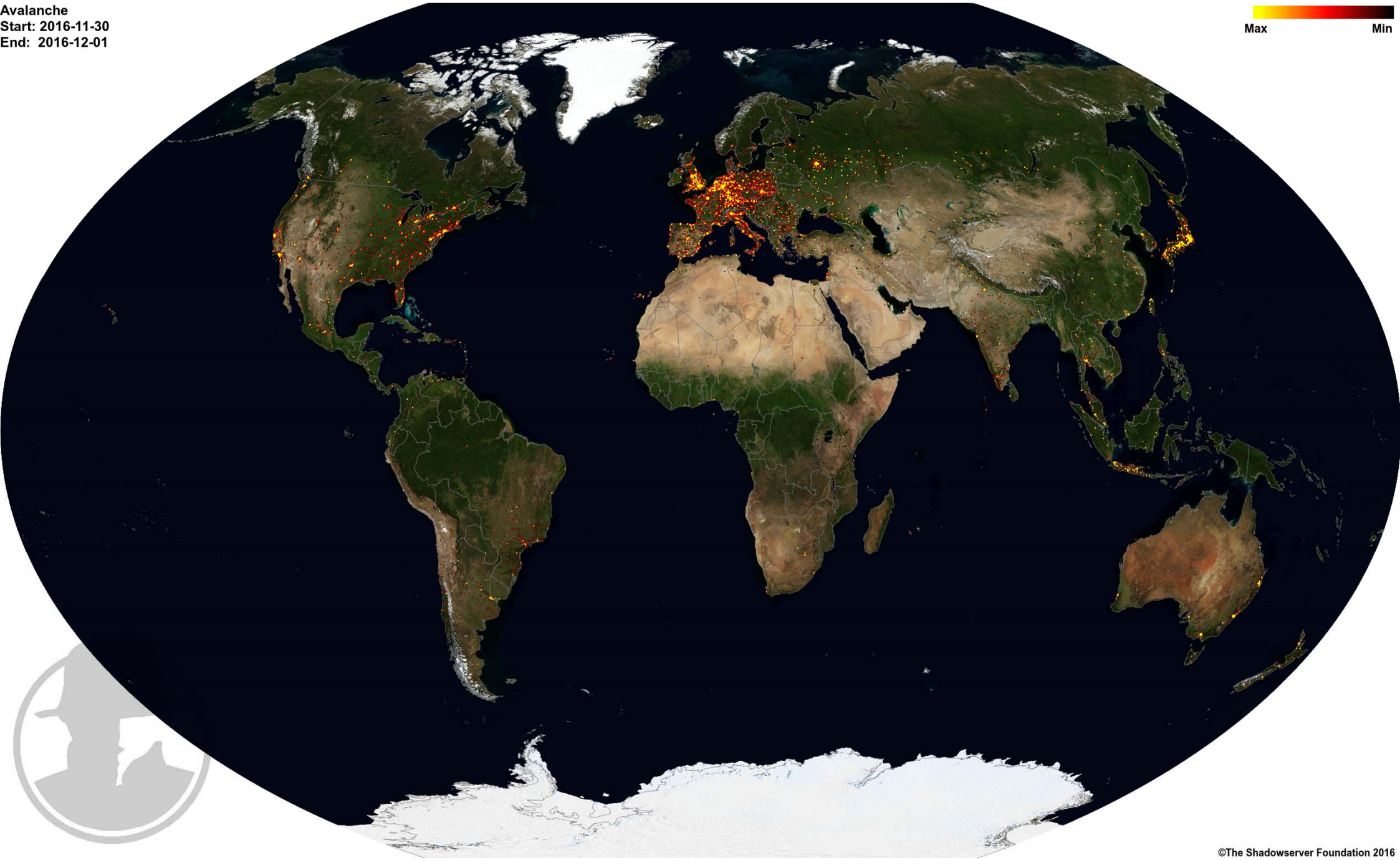
„Die ermittelten Täter agierten weltweit, waren untereinander vernetzt und arbeiteten arbeitsteilig hochprofessionell mit dem Ziel auf illegale Weise sehr viel Geld zu verdienen. Dabei nutzten sie bewusst den virtuellen Raum der keine nationalen Grenzen kennt. Im Rahmen dieses Verfahrens konnte eine nationale und internationale Kooperation initiiert werden, die es ermöglichte, die zur Bekämpfung dieses Deliktsfeldes erforderlichen Kompetenzen und Kräfte zu bündeln. Hierdurch erst war es möglich, professionelle Täter aus der vermeintlichen Anonymität des Internet heraus zu holen und die seit 2009 bestehende Botnetzinfrastruktur Avalanche unschädlich zu machen. Derartige Kooperationen dürften meines Erachtens richtungsweisend und erfolgsmaßgeblich für zukünftige derartige Ermittlungsverfahren sein.“

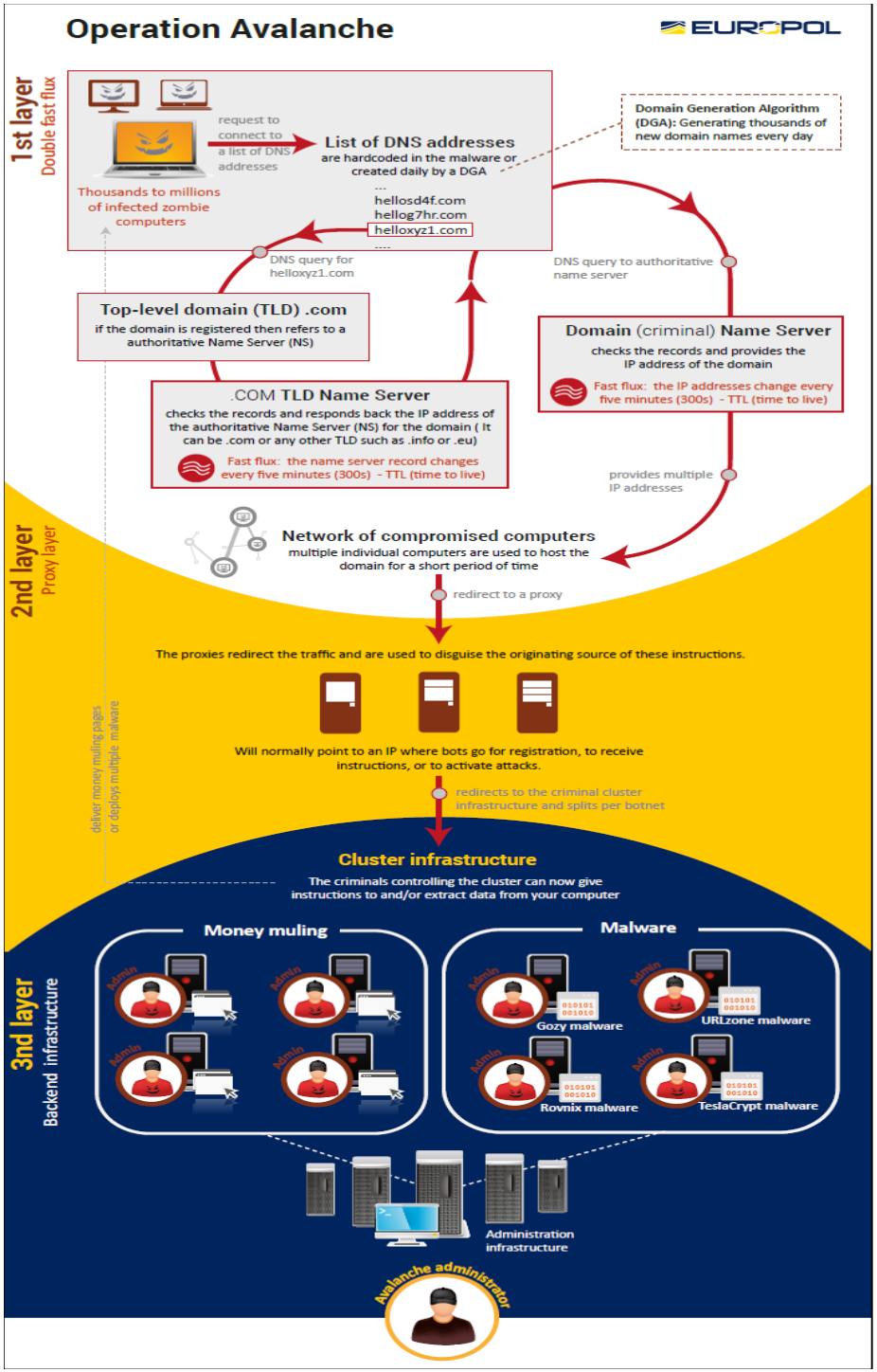
Leitender Oberstaatsanwalt Christian Schierholt, GenStA Celle – ZOK –:

"Nationale Strafverfahren stoßen bei der Bekämpfung der Kriminalität im Internet schnell an ihre nationalen Grenzen. Auch die Unterstützung durch die Behörden anderer Länder im Rahmen klassischer Rechtshilfe ist regelmäßig nicht mehr ausreichend. Eine effektive Strafverfolgung kann nur im Rahmen eines international arbeitsteiligen Ermittlungsverfahrens - unter Beachtung der jeweiligen nationalen Verfahrensrechte - erfolgreich sein. Das vorliegende Verfahren ist ein Musterbeispiel für eine solche konzertierte Ermittlung unter der Leitung der Staatsanwaltschaft Verden. Die Institutionen der Europäischen Union, Europol und Eurojust wie auch das Europäische Justizielle Netz waren frühzeitig eingebunden und haben die Koordinierung maßgeblich unterstützt. Die Zentrale Stelle Organisierte Kriminalität und Korruption, zu deren Aufgaben auch die Bekämpfung der Internetkriminalität gehört, hat das Verfahren ebenfalls unterstützend begleitet."

Es gilt das gesprochene Wort!

Avalanche
Start: 2016-11-30
End: 2016-12-01





Sinkholing
(Beschlagnahme aktuell genutzter und Umleitung zukünftiger Domains)

Information
(der infizierten Systeminhaber)

Abusemeldungen

Takedown

(Beschlagnahme der Server)

„Klassische“ strafprozessuale Maßnahmen

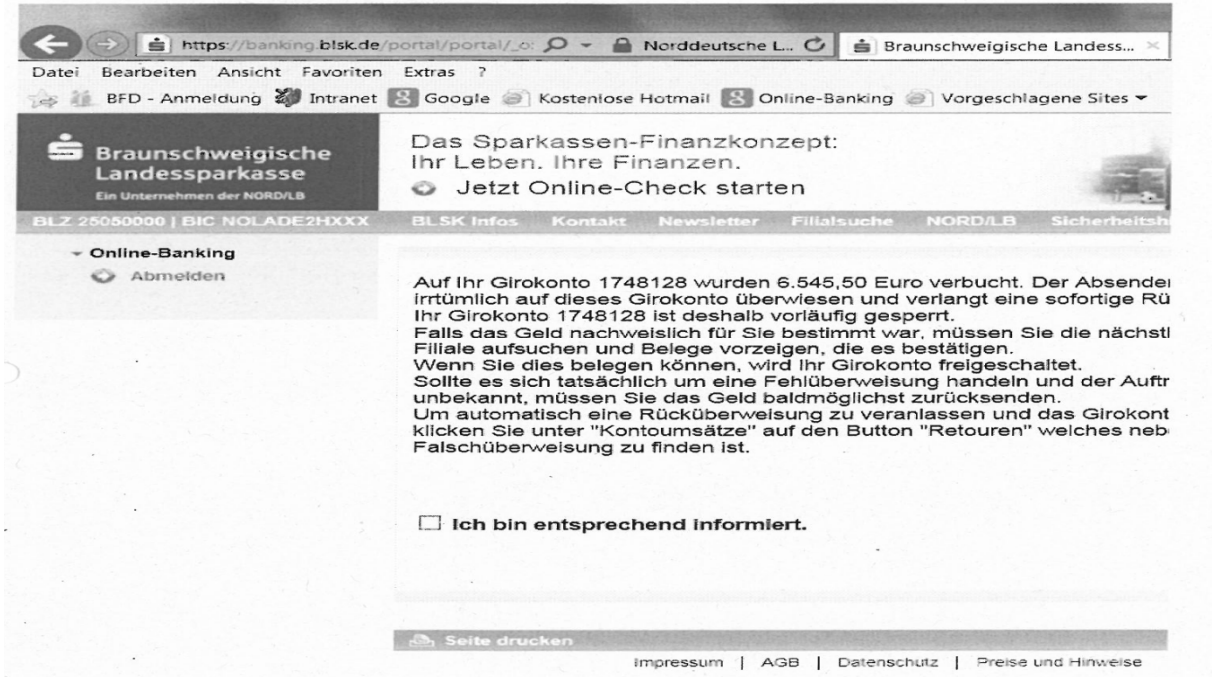
(Ermittlung der Täter, u. a. Durchsuchungen, Festnahmen, Vermögensab-schöpfung)

ZKI LÜNEBURG

StA VERDEN

Windowsverschlüsselungstrojaner (WVT)

„UrlZone“ (Bankingtrojaner)



Bundesamt
für Sicherheit in der
Informationstechnik

Pressemitteilung

HAUSANSCHRIFT
Godesberger Allee 185 - 189
53175 Bonn

TEL +49 (0) 22899 9582 - 5777
FAX +49 (0) 22899 9582 - 5400

presse@bsi.bund.de
www.bsi.bund.de

Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen

16 Millionen Digitale Identitäten betroffen

Bonn, 21. Januar 2014. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat angesichts eines Falles von großflächigem Identitätsdiebstahl unter https://www.sicherheitstest.bsi.de eine Webseite eingerichtet, auf der Bürgerinnen und Bürger überprüfen können, ob sie von diesem Identitätsdiebstahl betroffen sind. Im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden wurden rund 16 Millionen kompromittierte Benutzerkonten entdeckt. Diese bestehen in der Regel aus einem Benutzernamen in Form einer E-Mail-Adresse und einem Passwort. Viele Internetnutzer verwenden diese Login-Daten nicht nur für das eigene Mail-Account, sondern auch für Benutzerkonten bei Internetdiensten, Online-Shops oder Sozialen Netzwerken. Die E-Mail-Adressen wurden dem BSI übergeben, damit Betroffene informiert werden und erforderliche Schutzmaßnahmen treffen können.

Auf der Webseite https://www.sicherheitstest.bsi.de, die das BSI mit Unterstützung der Deutschen Telekom eingerichtet hat, können Internetnutzer ihre E-Mail-Adresse eingeben, um zu überprüfen, ob sie von dem Identitätsdiebstahl betroffen sind. Die eingegebene Adresse wird dann in einem technischen Verfahren vom BSI mit den Daten aus den Botnetzen abgeglichen. Ist die Adresse und damit auch die Digitale Identität des Nutzers betroffen, so erhält dieser eine entsprechende Information per E-Mail an die angegebene Adresse. Diese Antwort-Mail enthält auch Empfehlungen zu erforderlichen Schutzmaßnahmen. Ist die eingegebene E-Mail-Adresse nicht betroffen, so erhält der Nutzer keine Benachrichtigung.

Betroffene sollten Rechner säubern und Passwörter ändern

Betroffene Internetnutzer sollten in jedem Falle zwei Maßnahmen ergreifen:

1. Der eigene Rechner ebenso wie andere genutzte Rechner sollten auf Befall mit Schadsoftware überprüft werden. In den Empfehlungen des BSI zur sicheren Konfiguration von Windows-PCs ist eine Auswahl an geeigneten Virenschutzprogrammen aufgeführt, die hierfür genutzt werden können.

2. Anwender sollten alle Passwörter ändern, die sie zur Anmeldung bei Sozialen Netzwerken, Online-Shops, E-Mail-Accounts und anderen Online-Diensten nutzen. Es sollten auch diejenigen Passwörter geändert werden, die nicht zusammen mit der betroffenen E-Mail-Adresse als Login genutzt werden. Dies ist deshalb empfehlenswert, weil im Falle einer Betroffenheit die Möglichkeit besteht, dass ein benutzter Rechner mit einer Schadsoftware infiziert ist. Diese kann neben den in den Botnetzen aufgetauchten Benutzerkennungen auch andere Zugangsdaten, Passwörter oder sonstige Informationen des Nutzers ausgespäht haben. Hinweise zur Nutzung sicherer Passwörter erhalten Anwender unter https://www.bsi-fuer-buerger.de/Passwoerter

Identitätsdiebstahl gehört zu den Top-Gefährdungen im Internet

Identitätsdiebstahl ist eines der größten Risiken bei der Internetnutzung. Online-Kriminelle stehlen die digitalen Identitäten von Internetnutzern, um in deren Namen aufzutreten, E-Mails zu versenden, auf fremde Kosten in einem Online-Shop einzukaufen oder sich auf andere Weise zu bereichern oder den Betroffenen zu schaden. Personenbezogene Anwendungen wie E-Mail- oder Messenger-Dienste, Online-Shops oder Soziale Netzwerke bieten personalisierte Services, für die man sich anmelden muss, um seine Daten zu erhalten oder die Dienstleistung in Anspruch nehmen zu können. Zur Authentisierung wird in den meisten Fällen immer noch die Kombination aus Benutzername und Passwort genutzt. Geraten diese Authentisierungsmerkmale in die falschen Hände, können sie für Identitätsmissbrauch verwendet werden.

Meist geschieht dies durch eine Schadsoftware-Infektion des genutzten Internet-Rechners. Die Schadprogramme werden unbemerkt auf den Rechnern der Anwender platziert, um beispielsweise Tastatureingaben und Anmeldevorgänge zu protokollieren oder Transaktionen direkt zu manipulieren. Die protokollierten Daten werden dann vom Nutzer unbemerkt an speziell vom Angreifer dafür präparierte Rechner im Internet („Dropzones“) gesendet, von wo sie von den Tätern heruntergeladen und missbraucht werden können.

Pressekontakt:
Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi.fuer.buerger

Bundesamt
für Sicherheit in der
Informationstechnik

Pressemitteilung

HAUSANSCHRIFT
Godesberger Allee 185 - 189
53175 Bonn

TEL +49 (0) 22899 9582 - 5777
FAX +49 (0) 22899 9582 - 5400

presse@bsi.bund.de
www.bsi.bund.de

Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene

Bonn, 7. April 2014. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert angesichts eines erneuten Falles von großflächigem Identitätsdiebstahl betroffene Bürgerinnen und Bürger in Deutschland. Die Staatsanwaltschaft Verden (Aller) hat dem BSI einen Datensatz mit rund 21 Millionen E-Mail-Adressen und Passwörtern zur Verfügung gestellt. Nach technischer Analyse und Bereinigung durch das BSI verblieben rund 18 Millionen von Identitätsdiebstahl betroffene E-Mail-Adressen, darunter rund 3 Millionen deutsche E-Mail-Adressen. Die Inhaber der E-Mail-Adressen werden vom BSI in Zusammenarbeit mit den Online-Dienstleistern Deutsche Telekom, Freenet, gmx.de, Kabel Deutschland, Vodafone und web.de informiert. Zudem stellt das BSI wieder einen webbasierten Sicherheitstest zur Verfügung.

Die digitalen Identitäten sind im Rahmen eines laufenden Ermittlungsverfahrens gefunden worden. Mit den E-Mail-Adressen und den zugehörigen Passwörtern versuchen Kriminelle mithilfe eines Botnetzes, sich in E-Mail-Accounts einzuloggen und diese für den Versand von SPAM-Mails zu missbrauchen. Das Botnetz ist noch in Betrieb, die gestohlenen Identitäten werden aktiv ausgenutzt. Es ist davon auszugehen, dass es sich bei den gefundenen Adressen und Passwörtern sowohl um Zugangsdaten zu E-Mail-Konten als auch um Zugangsdaten zu anderen Online-Accounts wie Online Shops, Internet-Foren oder Sozialen Netzwerken handelt.

Information per E-Mail und Prüfmöglichkeit auf Internetseite

Aufgrund dieser aktuellen Ausnutzung der Daten erfolgt die Information der Betroffenen in Deutschland in einem zweigeteilten, datenschutzkonformen Verfahren unter Beteiligung der Online-Dienstleister Deutsche Telekom, Freenet, gmx.de, Kabel Deutschland, Vodafone und web.de. Das BSI hat diesen Providern die in ihren Domänenbereich fallenden E-Mail-Adressen zur Verfügung gestellt, damit diese im Rahmen ihrer bestehenden Kundenbeziehungen ihre Kunden informieren. Hierbei handelt es sich um ein datenschutzgerechtes Verfahren zur Warnung vor IT-Risiken, mit dem im vorliegenden Fall bereits rund 70 Prozent der Betroffenen in Deutschland abgedeckt werden können.

Internetnutzer, die ein E-Mail-Account bei einem anderen als den oben genannten Dienstleistern haben oder einen eigenen Webserver betreiben, sind aufgerufen, mithilfe des vom BSI bereitgestellten webbasierten Sicherheitstests unter https://www.sicherheitstest.bsi.de zu überprüfen, ob sie von dem erneuten Identitätsdiebstahl betroffen sind. Der neue Datensatz wurde in den seit Januar bestehenden Sicherheitstest eingepflegt. Die eingegebene Adresse wird in einem technischen Verfahren vom BSI mit den Daten abgeglichen, die die Staatsanwaltschaft Verden (Aller) zur Verfügung gestellt hat. Ist die Adresse und damit auch die digitale Identität des Nutzers betroffen, so erhält dieser eine entsprechende Information per E-Mail an die angegebene Adresse. Ist die eingegebene E-Mail-Adresse nicht betroffen, so erhält der Nutzer keine Benachrichtigung.

Betroffene sollten Rechner bereinigen und Passwörter ändern

Das BSI geht derzeit davon aus, dass sich die Online-Kriminellen verschiedener Quellen bedient haben, um an die Zugangsdaten zu gelangen. Eine dieser möglichen Quellen sind die Rechner von Internetnutzern, zu denen sich die Angreifer Zugriff verschafft haben können. Dazu wird der Rechner in der Regel mit einer Schadsoftware infiziert, die dann die Eingabe der Zugangsdaten mitliest. Es ist nicht auszuschließen, dass diese Schadsoftware auch zu anderen Zwecken genutzt werden kann, etwa zur Ausspähung weiterer Daten auf dem Computer oder zur Manipulation von Online-Transaktionen, die die Anwender etwa beim Online-Shopping durchführen.

Betroffene, die von ihrem Provider informiert wurden oder ihre Betroffenheit über den webbasierten Sicherheitstest herausgefunden haben, erhalten mit der Information daher auch Empfehlungen zu erforderlichen Bereinigungs- und Schutzmaßnahmen:

1. Der eigene Computer ebenso wie andere genutzte Rechner sollten mit einem Virenschutzprogramm auf Befall mit Schadsoftware überprüft und bereinigt werden. Als zusätzliche Möglichkeit der Überprüfung kann der „PC-Cleaner" verwendet werden, zu dem auf der auf der Webseite „BSI für Bürger“ verlinkt ist.
2. Nach der Überprüfung und Bereinigung des Rechners sollten Anwender ihr E-Mail-Passwort sowie auch alle anderen Passwörter ändern, die sie zur Anmeldung bei Sozialen Netzwerken, Online-Shops und anderen Online-Diensten nutzen.
3. Um generell zu verhindern, dass Schadsoftware auf den Rechner gelangt, sollten Anwender die grundlegenden Sicherheitsregeln beachten, die das BSI auf seiner Webseite „BSI für Bürger“ zusammengestellt hat.
4. Anwender sollten zukünftig in regelmäßigen Abständen überprüfen, ob ihr Computer verwundbar für Angriffe aus dem Internet ist. Eine schnelle Testmöglichkeit bietet das Angebot „Check and Secure“ der Initiative botfrei.de des eco-Verbands.

Häufige Fragen

1. Ich habe von der Abschaltung der Avalanche-Botnetzinfrastruktur gehört. Was bedeutet das?

Eine international agierende Tätergruppierung hat eine Infrastruktur für Botnetze aufgebaut, über die millionenfach private und geschäftliche Computersysteme und Mobilgeräte mit unterschiedlicher Schadsoftware infiziert wurden. Ca. 20 verschiedene Botnetze nutzten diese Infrastruktur, um u.a. Spam- und Phishing-E-Mails zu versenden, Ransomware (Erpressungstrojaner) zu verbreiten und die Nutzer von Online-Banking-Angeboten zu betrügen. Nähere Informationen finden Sie dazu in der gemeinsamen Pressemitteilung der Staatsanwaltschaft Verden (Aller), der Zentralen Kriminalinspektion Lüneburg (ZKI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

2. Ich habe eine Benachrichtigung von meinem Provider erhalten. Woher weiß dieser, dass ich betroffen bin?

Im Rahmen der Zerschlagung werden sogenannte Sinkhole-Server eingesetzt, zu denen die Verbindungsversuche infizierter Systeme umgeleitet werden. Sie dienen dazu, diese Verbindungsversuche aufzuzeichnen. Auf diesem Weg erhält das BSI die IP-Adressen dieser Systeme. Da den Internetserviceprovidern feste Adressbereiche zugeordnet sind, kann das BSI die in ihrem Adressbereich befindlichen IP-Adressen gezielt an die Provider melden. Diese sind dann in der Lage, die betroffenen Kunden zu identifizieren und zu warnen. Dies ist notwendig, da die Identifizierung der Kunden technisch ausschließlich durch die Internetserviceprovider erfolgen kann. Dem BSI liegen keine Kundendaten vor, eine direkte Warnung durch das BSI kann daher nicht erfolgen.

3. Ich habe eine Benachrichtigung von meinem Provider erhalten. Was soll ich tun?

Die Benachrichtigung bedeutet, dass zu dem von Ihrem Provider angegebenen Zeitpunkt an Ihrem Netzwerkanschluss ein Gerät Teil der Avalanche-Infrastruktur war und vermutlich immer noch ist.

Das BSI empfiehlt betroffenen Anwendern in diesem Fall, grundsätzlich alle am Netzwerkanschluss genutzten Computer oder Mobilgeräte auf Befall mit Schadsoftware zu überprüfen und Sicherheitslücken zu schließen. Es wurde festgestellt, dass die Täter in der Avalanche-Botnetzinfrastruktur hauptsächlich Schadsoftware auf Rechnern mit Windows-Betriebssystem platziert haben. Daneben wurden aber auch Schadsoftwarefamilien identifiziert, die auf Smartphones und Tablets mit Android zum Einsatz kommen. Dennoch ist nicht auszuschließen, dass Schadsoftware auch unter anderen Betriebssystemen eingesetzt wurde.

Sofern Ihr Provider angegeben hat, um welche Schadsoftware es sich handelt, können Sie unter Frage 17 weitergehende Informationen zu den bisher bekannten der bei Avalanche eingesetzten Schadprogramme und einer empfohlenen Vorgehensweise erhalten.

Nach einer Bereinigung der Rechner und Mobilgeräte empfiehlt das BSI alle Passwörter zu ändern, die Sie für Ihren Mail-Account und andere Benutzerkonten bei Online-Shops, Sozialen Netzwerken oder weiteren Internetdiensten nutzen. Wichtig: Überprüfen und bereinigen Sie zuerst Ihre Systeme und ändern Sie danach Ihre Passwörter! Andernfalls kann eine eventuelle Schadsoftware auch die neuen Passwörter mitlesen.

Achten Sie bei der Änderung darauf, dass Sie ein möglichst sicheres Passwort wählen und nicht für jeden Dienst das gleiche Passwort nutzen. Empfehlungen hierzu gibt das BSI unter www.bsi-fuer-buerger.de/Passwoerter. Zur Prüfung auf Schadsoftwarebefall gibt es eine Reihe von Virenschutzprogrammen. Weitere Informationen rund um die Bereinigung von infizierten Rechnern finden Sie hier auf bsi-fuer-buerger.de sowie auf den Seiten des Anti-Botnet Beratungszentrums. Sollte Ihr Virenschutzprogramm keine Infektion finden, empfiehlt sich der Einsatz einer Virenschutz-Boot-CD, beispielsweise das Antibot Rettungssystem, welches vom Anti-Botnetz-Beratungszentrum angeboten wird. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Betriebssystem neu installieren.

Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps. Tipps zum Schutz Ihres Smartphones oder Tablets finden Sie unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

4. Erkennt mein Virenschutzprogramm die über die Avalanche-Botnetze verteilte Schadsoftware?

In dieser Liste sind die Hersteller aufgeführt, deren Produkte nach Herstelleraussage einen großen Teil der Schadsoftware von Avalanche erkennen können. Das BSI hat nicht überprüft, ob und welchem Umfang dies zutreffend ist. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

Durch die ständige Weiterentwicklung der Schadsoftware ist nicht gewährleistet, dass alle Infektionen von den nachfolgenden Herstellern garantiert erkannt werden können.

Avira	PC Cleaner
Bit Defender	Bitdefender Removal Tool (englisch)
Dr. Web	Dr. Web CureIt!
ESET	ESET Online Scanner
F-Secure	F-Secure Online Scanner
G-Data	

Kaspersky	Kaspersky Total Security Kaspersky Rescue Disk
McAfee	McAfee Stinger (englisch)
Symantec/Norton	Norton Power Eraser
TrendMicro	HouseCall

Diese Liste wird erweitert.

Weitere Informationen rund um die Säuberung von infizierten Rechnern finden Sie hier auf bsi-fuer-buerger.de sowie auf den Seiten des Anti-Botnet Beratungszentrums.

5. Ich habe keine Benachrichtigung meines Providers erhalten. Bedeutet dies, dass mein Rechner frei von Schadsoftware ist?

Nein, leider bedeutet es das nicht automatisch. Falls Sie keine Benachrichtigung durch den Provider erhalten haben, bedeutet dies nur, dass die IP-Adresse Ihres Netzwerkanschlusses im Rahmen der Abschaltung der Botnetz-Infrastruktur nicht bekannt wurde oder Ihr Provider Sie noch nicht informiert hat. Das BSI informiert die Provider über die ihnen zugeordneten IP-Adressen infizierter Systeme. Die Zuordnung, welcher Kunde des Providers betroffen ist und die Entscheidung wann dieser informiert wird, erfolgt durch den Internet-Serviceprovider.

Es gibt neben der in der Avalanche-Botnetzinfrastruktur eingesetzten Schadsoftware eine Vielzahl von Schadsoftware sowie viele weitere Botnetze, die auch weiterhin aktiv sind. Um eine mögliche Infektion zu erkennen, können Sie eine vollständige Untersuchung ihres Systems mit einem Virenschutzprogramm durchführen. Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Empfehlungen des BSI unter 12 Sicherheitststipps.

6. Wie wurde mein Rechner infiziert?

Die Schadprogramme der Avalanche-Botnetzinfrastruktur wurden typischerweise per E-Mail verbreitet. Diese enthielten oftmals eine persönliche Ansprache (Name und teilweise auch Vorname oder Nickname des E-Mail-Empfängers) und einen infizierten Dateianhang. Im Text dieser Spam-Mails wurde dem Empfänger z.B. mitgeteilt, dass durch Vertragsabschlüsse, Mitgliedschaften, Onlinekäufe oder ähnliches Kosten in empfindlicher Höhe entstanden seien. In den unaufgefordert übersandten E-Mails befanden sich in der Regel Anhänge im „ZIP-Format“, die eine Rechnung/Abmahnung für den genannten Kauf, die Mitgliedschaft oder ähnliches enthielten. Im Anhang befand sich dann jedoch meist ein sogenannter Downloader, der Kontakt zu einem Steuerungsserver aufgenommen und von dort Schadsoftware heruntergeladen hat.

Grundsätzlich kann Schadsoftware auch über andere Verbreitungswege auf Ihr System gelangen [https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme /schadprogramme_node.html].

7. Was bedeutet es, wenn mein Computer oder Smartphone Teil eines Botnetzes ist?

Die Infektion des Computers oder Smartphones mit Schadsoftware führt oft dazu, dass das System zum Teil eines Botnetzes wird. Mit dem Begriff Bot ist dabei ein Schadprogramm gemeint, welches einem Angreifer die Fernsteuerung des infizierten Gerätes ermöglicht. Von Botnetzen spricht man, wenn sehr viele Geräte (meist mehrere Tausend) per Fernsteuerung zusammengeschlossen werden. Botnetze werden dazu eingesetzt, vertrauliche Daten wie Passwörter, Online-Banking-Daten oder Geschäftsinformationen zu stehlen. Botnetze dienen auch dazu, verteilte Angriffe auf die Verfügbarkeit von Internetsystemen (sogenannte Distributed Denial of Service oder kurz DDoS-Angriffe) durchzuführen. Aufgrund ihrer vielfältigen Einsatzmöglichkeiten und der wirtschaftlich motivierten kriminellen Energie, welche die Täter aufbringen, stellen Botnetze derzeit eine der größten Gefahren im Internet dar. Über gefälschte/ manipulierte Internetseiten oder wie im Fall Avalanche, über Phishing-Angriffe mit gefälschten E-Mails, können Daten in falsche Hände gelangen oder auch Identitäten gestohlen werden.
Wie ein Botnetz funktioniert haben wir für Sie in einem kurzen Video erklärt. [https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/botnetze_node.html]

Ist mir bereits ein Schaden entstanden, ohne dass ich es bemerkt habe?

Das ist möglich. Die von den Tätern eingesetzte Schadsoftware eröffnet eine Vielzahl von Möglichkeiten, auf den infizierten PC zuzugreifen. Etwa zur Ausspähung weiterer Daten auf Ihrem Computer oder zur Manipulation von Online-Transaktionen, die Sie bei Online-Shops oder im Rahmen des Online-Bankings durchführen.

Deshalb sollten Sie in regelmäßigen Abständen anhand eines Kontoauszugs etwa in Papierform prüfen, ob Ihnen verdächtige Kontobewegungen auffallen. Beispielsweise ist die in Avalanche eingesetzte Schadsoftware URLzone in der Lage, die Anzeige des Bankkontostandes im Internet-Browser zu manipulieren, so dass eine Prüfung per Internet-Browser kein verlässliches Ergebnis liefert. Wir haben für Sie Informationen zu sicherem Online-Banking zusammengestellt. [https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/onlinebanking_node.html]

8. Mein Virenschutzprogramm zeigt nach einem Scan oder einer Bereinigung keine Infektion an. Ist mein System nun sicher?

Eine 100%-ige Garantie für eine erfolgreiche Bereinigung durch ein Anti-Virenprogramm ist nicht möglich, da die Angreifer regelmäßig die eingesetzte Software anpassen. Untersuchungen zeigen, dass befallene Systeme häufig mit mehreren Schadprogrammen infiziert sind. Es ist daher wichtig, nach einer Benachrichtigung durch den Provider Ihre Geräte anhand eines geeigneten Virenschutzprogramms sorgfältig auf Befall zu prüfen.

Sollten Sie Zweifel haben, dass die Bereinigung erfolgreich war, empfiehlt es sich sicherheitshalber, nach einem Backup der Daten das System zu löschen und neu aufzusetzen. Beachten Sie bitte dabei, dass Sie aus dem Backup keine ausführbaren Programme wiederherstellen, da diese mit der Schadsoftware befallen sein könnten. Ziehen Sie im Zweifel einen Computer-Spezialisten hinzu.

Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps.

9. Sind Geräte des Internets der Dinge (Internet of Things, IoT) wie beispielsweise Webcams, Drucker oder TV-Empfänger betroffenen?

Bei der analysierten Botnetz-Infrastruktur konnten keine IoT-Botnetze identifiziert werden. Nach aktuellem Kenntnisstand des BSI sind vorrangig Windows-Systeme und Android-Geräte betroffen.

10. Was ist der Unterschied zwischen einer Botnetzinfrastruktur und einem Botnetz?

Eine Botnetzinfrastruktur wird von Kriminellen als redundante Infrastruktur zum Betrieb von Botnetzen angeboten. Sie ermöglicht es den Tätern, ihre auf vielen tausend Geräten verteilten Bots (das Botnetz) zu steuern ohne eine Vielzahl von eigenen Servern betreiben zu müssen.

11. Warum könnten einzelne Botnetze trotz des Aushebens der Infrastruktur wieder aktiv werden?

Die Botnetzinfrastruktur wurde zwar abgeschaltet, die Bots selbst bleiben aber bis zu einer Bereinigung durch den Nutzer auf den Geräten. Falls es den Tätern gelingt, eine alternative Botnetzinfrastruktur aufzubauen, könnten diese Bots erneut ferngesteuert werden. Daher ist es wichtig, diese Bots zügig von betroffenen Geräten zu entfernen.

12. Mein Provider hat in seinem Anschreiben den Namen einer Schadsoftware genannt, mein Virenschutzprogramm findet aber nur Schadsoftware mit anderem Namen. Was bedeutet das?

Die Hersteller von Virenschutzprogrammen benennen Schadsoftware von Botnetzen nicht einheitlich. Eine Zuordnung von Schadprogrammen zu Botnetznamen ist zudem sehr aufwändig und nicht immer eindeutig, da manche Schadprogramme als sogenannte Downloader nur zum Nachladen weiterer Schadprogramme genutzt werden. Häufig ist auf infizierten Rechnern zudem Schadsoftware für mehrere Botnetze zu finden. Daher werden bei Funden häufig generische Namen wie z.B. „Downloader.XYZ“ angezeigt.

13. Was hat dies mit gestohlenen Identitäten zu tun?

Beim dem aktuellen Takedown der Avalanche-Botnetzinfrastruktur handelt es sich nicht um einen Datenfund gestohlener Identitäten. Beim der Zerschlagung der Avalanche-Botnetzinfrastruktur werden die Bürger direkt von Ihren Providern informiert, sofern ihre Rechner aktuell infiziert sind.

14. Ich habe mein System bereinigt oder neu aufgesetzt, erhalte nun aber eine zweite Benachrichtigung durch meinen Provider. Muss ich erneut tätig werden?

Ja. Erhalten Sie eine erneute Meldung durch Ihren Provider ist Ihr System oder Ihr Smartphone erneut oder immer noch mit Schadsoftware infiziert. Dies kann beispielsweise folgende Gründe haben:

- Ihre Bereinigung war nicht erfolgreich oder nicht vollständig. Es empfiehlt sich, das System neu aufzusetzen. Im Zweifel sollten Sie einen Computer-Spezialisten hinzuziehen.
- Ihr System wurde erneut mit Schadsoftware infiziert. Bitte beachten Sie unsere Tipps zum Schutz Ihres Systems [https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html] und unsere Hinweise zum sicheren Surfen im Internet.
- Ein anderes System an Ihrem Netzwerkanschluss ist immer noch oder erneut mit Schadsoftware infiziert.

15. Erhalte ich nun jedes Mal, wenn mein System mit Schadsoftware infiziert ist, eine Benachrichtigung?

Nein. Sie erhalten nur dann eine Benachrichtigung, wenn Ihr System mit Schadsoftware infiziert ist, die mit Sinkholes der abgeschalteten Avalanche-Botnetzinfrastruktur oder mit anderen Sinkholes kommuniziert, deren Informationen das BSI erhält. Schadsoftware, die aus anderen Quellen stammt, wird

davon nicht erfasst, daher erhalten Sie darüber auch keine Benachrichtigung.

Um generell zu verhindern, dass Schadsoftware auf Ihren Rechner gelangen kann, beachten Sie bitte die Hinweise und Empfehlungen des BSI unter 12 Sicherheitstipps.

16. Was ist ein Sinkhole-Server?

Ein gängiges Verfahren zur Identifikation mit Schadprogrammen infizierter Systeme ist die Umleitung von Steuerungsdomänennamen auf sogenannte "Sinkholes". Dabei werden die durch Analyse von Schadprogrammen ermittelten Domainnamen, mit denen die Schadprogramme kommunizieren, in Zusammenarbeit mit den zuständigen Domain-Registrierungsstellen auf Sinkhole-Server umgeleitet. Die Sinkholes protokollieren anschließend die Zugriffe auf die schädlichen Domainnamen mit Zeitstempel und der Quell-IP-Adresse sowie Quell-Port, von welcher der Zugriff erfolgte. Solche Sinkholes werden von zahlreichen Analysten und IT-Sicherheitsdienstleistern weltweit betrieben.

Da sich unter den Domainnamen keine legitimen Internetangebote befinden, werden diese üblicherweise nicht angesteuert. Ein Zugriff auf einen solchen Domainnamen ist daher ein gutes Indiz, dass sich unter der Quell-IP-Adresse, von welcher ein Zugriff erfolgt, mit hoher Wahrscheinlichkeit ein mit einem entsprechenden Schadprogramm infiziertes System befindet.

Die von den Sinkhole-Betreibern gelieferten Daten enthalten üblicherweise zu jedem protokollierten Zugriff einen Zeitstempel, die Quell-IP-Adresse, den aufgerufenen schädlichen Domainnamen und eine Bezeichnung des damit verbundenen Schadprogramms, welches den Domainnamen für die Kontaktaufnahme zu einem Kontrollserver verwendet. Häufig sind auch die IP-Adressen der Sinkholes sowie die Quell- und Ziel-Portnummern der Verbindung in den Daten enthalten.

17. Welche Schadsoftware wurde in der Avalanche-Botnetzinfrastruktur identifiziert?

Nachfolgend werden bekannte Botnetzfamilien (Schadsoftware) dargestellt, die in der Botnetzinfrastruktur Avalanche aufgefunden wurden. Bitte beachten Sie, dass die Hersteller von Virenschutzprogrammen die Botnetzfamilien nicht einheitlich benennen. Häufig werden bei Funden auch generische Namen wie z.B. „Downloader.XYZ“ angezeigt.

17.1 Andromeda/Gamarue

Andromeda/Gamarue ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Andromeda/Gamarue können dies z.B. die Banking-Trojaner Citadel, Rovnix oder UrlZone/Bebloh sein. Des Weiteren ist Andromeda/Gamarue mit Hilfe von Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Andromeda/Gamarue infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Andromeda/Gamarue wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken im Browser durch präparierte Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Andromeda/Gamarue weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Durchsuchung ihres Systems mit einem Virenscanner durch. Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Andromeda/Gamarue zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten Systemalle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

17.2 Bolek

Bolek ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Bolek zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Bolek infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch.Es kann sich zusätzlich zu Bolek auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.3 Citadel

Citadel ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Citadel zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Citadel infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Citadel auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann

17.4 Corebot

Corebot ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Corebot zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Corebot infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Corebot auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.5 Dofoil/Smokeloader

Dofoil/Smokeloader ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Dofoil/Smokeloader kann dies z.B. die Schadsoftware Matsnu sein. Des Weiteren ist Dofoil/Smokeloader mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Dofoil/Smokeloader infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Dofoil/Smokeloader wird von den Tätern getarnt als Rechnung per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Dofoil/Smokeloader weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Dofoil/Smokeloader zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

17.6 Gozi2

Gozi2 ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Gozi zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Gozi2 infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Gozi auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit

ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.7 KINS/VMZeus

KINS/VMZeus ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann KINS/VMZeus zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit KINS/VMZeus infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu KINS/VMZeus weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen.

17.8 Marcher

Marcher ist ein Banking-Trojaner für Android-Geräte . Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Marcher werden SMS mit smsTAN/mTAN bgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Marcher infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren Windows-PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up-Fenster in ihrem Browser, mit der Aufforderung eine zusätzliche Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone oder Tablet durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie ihr Smartphone auf die Werkseinstellungen zurück. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.9 Matsnu

Matsnu ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Matsnu können dies z.B. die Banking-Trojaner Citadel und UrlZone/Bebloh sein.

Wie habe ich mich mit Matsnu infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Matsnu wird von den Tätern getarnt als Rechnung per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Matsnu weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

17.10 Nymaim

Nymaim ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Nymaim können dies z.B. die Banking-Trojaner Citadel und UrlZone/Bebloh sein. Des Weiteren ist Nymaim mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Nymaim infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Nymaim wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken in Browsern durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Nymaim weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegebenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Nymaim zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt

wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

17.11 Pandabanker

Pandabanker ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Pandabanker zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Pandabanker infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Pandabanker auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.12 Ranbyus

Ranbyus ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Ranbyus zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Ranbyus infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Ranbyus auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.13 Rovnix

Rovnix ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Rovnix zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen. Rovnix kann sich sehr tief im System verstecken, sodass eine Erkennung vom infizierten System aus nicht mit Sicherheit festgestellt werden kann.

Wie habe ich mich mit Rovnix infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Rovnix weitere Schadsoftware auf Ihrem System befinden. Nutzen Sie eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Rovnix zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem mit ihrer Bank in Kontakt, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.14 Smart App

Smart App ist ein Banking-Trojaner für Android-Geräte. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Smart App werden SMS mit smsTAN/mTAN abgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Smart App infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up Fenster in Ihrem Browser, mit der Aufforderung eine zusätzliche Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone oder Tablet durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie Ihr Smartphone auf die

Werkseinstellungen zurück. Sichern Sie vor einer Bereinigung Ihre persönlichen Daten. Ändern Sie auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.15 TeslaCrypt

TeslaCrypt ist ein Ransomware-Trojaner. Ransomware-Trojaner verschlüsseln Teile Ihrer Daten auf der Festplatte und erpressen dann Lösegeld für die Entschlüsselung dieser Daten.

Wie habe ich mich mit TeslaCrypt infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu TeslaCrypt auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann. Ein TeslaCrypt-Entschlüsselungswerkzeug wird von dem Europol-Projekt "No-More-Ransom" bereitgestellt (https://www.nomoreransom.org).

17.16 Tiny Banker/Tinba

Tiny Banker/Tinba ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab um, an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Tinba zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Tiny Banker/Tinba infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Tinba weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.17 Trusteer App

Trusteer App ist ein Banking-Trojaner für Android-Geräte . Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Im Fall von Trusteer App werden SMS mit smsTAN/mTAN abgefangen und an die Täter weitergeleitet.

Wie habe ich mich mit Trusteer App infiziert?

Ein möglicher Infektionsweg ist über eine weitere Schadsoftware, z.B. einen Banking-Trojaner wie URLZone/Bebloh, die bereits Ihren PC infiziert hat. Diese Schadsoftware öffnet z.B. beim Besuch einer Banking-Seite ein Pop-Up Fenster in ihrem Browser, mit der Aufforderung eine zusätzliche Sicherheitsanwendung auf ihrem Smartphone zu installieren. Alternativ kann Ihnen auch ein Link zu dieser Schadsoftware in einer SMS zugeschickt worden sein.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Smartphone durch. Nutzen Sie einen Virenscanner für Android oder setzen Sie ihr Smartphone auf die Werkseinstellungen zurück. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.18 URLzone/Bebloh

URLZone/Bebloh ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann URLZone/Bebloh zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit URLZone/Bebloh infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu URLZone/Bebloh weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie

vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.19 Vawtrak

Vawtrak ist ein Banking-Trojaner. Banking-Trojaner fangen die Kommunikation mit Ihrer Bank ab, um an PINs und TANs zu gelangen. Sie können Ihnen daher erheblichen finanziellen Schaden zufügen. Des Weiteren kann Vawtrak zusätzliche Zugangsdaten, z.B. von Ihrem E-Mail-Konto, abfangen.

Wie habe ich mich mit Vawtrak infiziert?

Ein möglicher Infektionsweg ist über weitere Schadsoftware, sogenannte Schadsoftware-Downloader, welche sich bereits auf Ihrem System befunden haben. Beispiele für solche Schadsoftware-Downloader sind Andromeda/Gamarue oder Matsnu.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Vawtrak auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung Ihre persönlichen Daten. Ändern Sie auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden. Sofern Sie Internet-Banking nutzen, treten Sie außerdem in Kontakt mit Ihrer Bank, damit diese entsprechende Sicherheitsmaßnahmen treffen kann.

17.20 Xswkit

Xswkit ist ein Malware-Downloader. Malware-Downloader laden weitere Schadsoftware nach und führen diese auf dem infizierten System aus. Im Falle von Xswkit können dies z.B. die Banking-Trojaner Citadel, Rovnix oder UrlZone/Bebloh sein. Des Weiteren ist Xswkit mit Plug-Ins um zusätzliche Funktionen erweiterbar. Es existiert unter anderem ein Plug-In, welches sowohl Zugangsdaten von E-Mail-Konten als auch von FTP-Programmen abfängt und an die Betreiber der Schadsoftware weiterleitet.

Wie habe ich mich mit Xswkit infiziert?

Ein möglicher Infektionsweg ist E-Mail-Spam. Xswkit wird von den Tätern, getarnt als Rechnung, per E-Mail versendet. Oftmals sind diese Rechnungen als ausführbare Dateien in ZIP-Archiven verpackt. Weitere mögliche Infektionswege sind die Ausnutzung von Sicherheitslücken im Browser durch bösartige Webseiten oder der Download durch eine weitere Schadsoftware, welche sich zu dem Zeitpunkt bereits auf Ihrem System befand.

Was muss ich jetzt machen?

Führen Sie keine sensiblen Transaktionen mehr auf Ihrem Computer durch. Es kann sich zusätzlich zu Xswkit nun auch weitere Schadsoftware auf Ihrem System befinden. Führen Sie in jedem Fall eine vollständige Überprüfung Ihres Systems mit einem Antivirenprogramm durch Nutzen Sie gegenenfalls eine Desinfektions-Live-CD, wie z.B. EU-Cleaner, um Xswkit zu entfernen. Bleiben Zweifel, dass die Infektion wirksam beseitigt wurde, sollten Sie das Gerät neu aufsetzen und das Betriebssystem neu installieren. Sichern Sie vor einer Bereinigung ihre persönlichen Daten. Ändern Sie des Weiteren auf dem bereinigten System alle Ihre Passwörter, da diese eventuell von den Tätern ausspioniert wurden.

Teilnehmerliste PK „AVALANCHE“

- Robert Kruse, Polizeipräsident, Polizeidirektion Lüneburg,
- Christian Schierholt, Leitender Oberstaatsanwalt,
  Generalstaatsanwaltschaft Celle - ZOK -,
- Stefan Mayer, Kriminaldirektor, ZKI Lüneburg,
- Stefanie Netzel-Huschebeck, Polizeioberkommissarin, ZKI Lüneburg ,
- Frank Lange, Oberstaatsanwalt, Staatsanwaltschaft Verden -
  Schwerpunktstaatsanwaltschaft zur Bekämpfung der IuK-Kriminalität,
- Arne Schönbohm, Präsident, Bundesamt für Sicherheit in der
  Informationstechnik,
- Dr. Lothar Eßer, Bundesamt für Sicherheit in der Informationstechnik,
  Leiter Referat C11 - Internetsicherheit -,
- Matthias Gärtner, Pressesprecher,
  Bundesamt für Sicherheit in der Informationstechnik,
- Lutz Gaebel, Pressesprecher, Staatsanwaltschaft Verden.