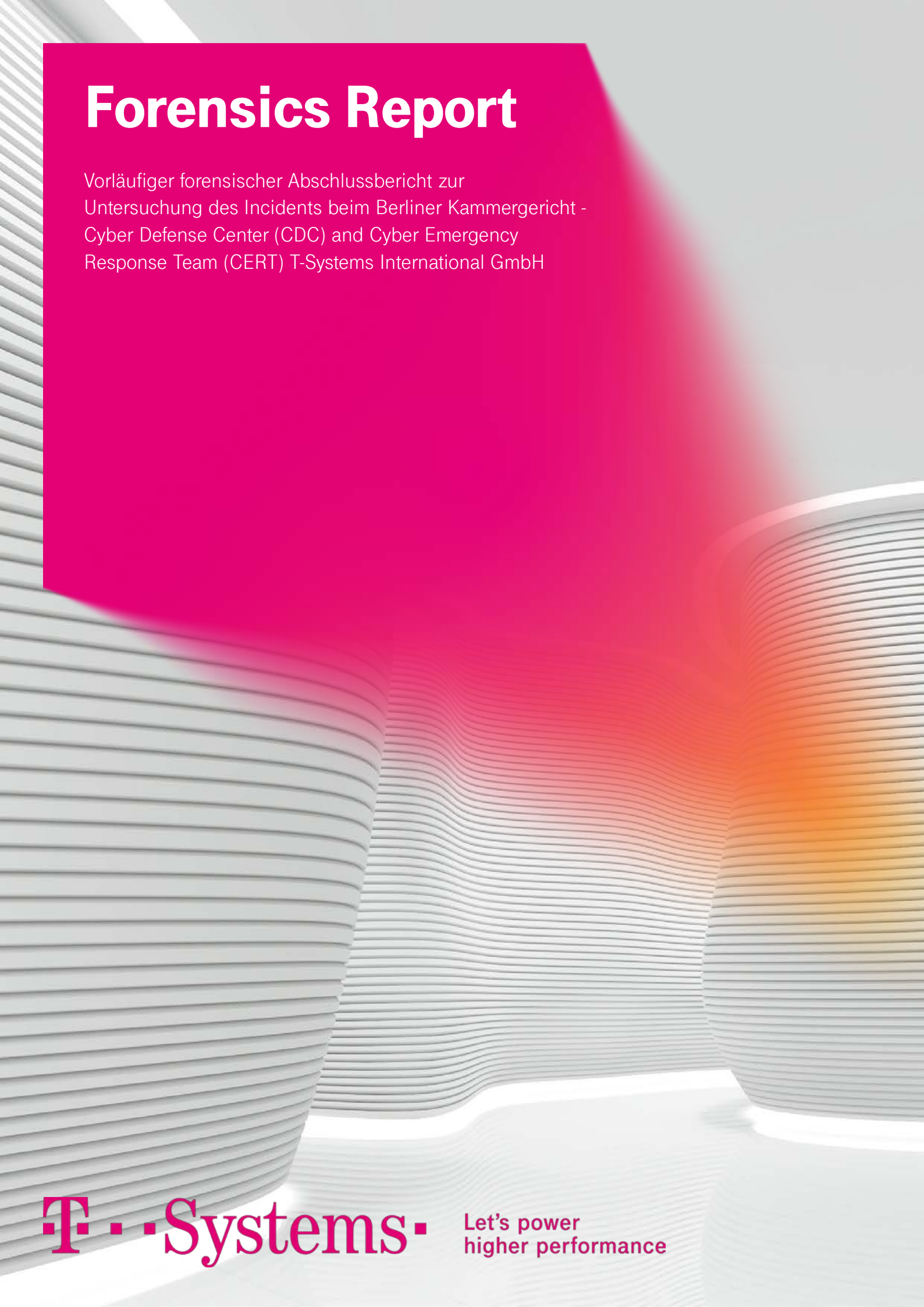
Forensics Report

Vorläufiger forensischer Abschlussbericht zur Untersuchung des Incidents beim Berliner Kammergericht - Cyber Defense Center (CDC) and Cyber Emergency Response Team (CERT) T-Systems International GmbH



T · · Systems ·

Let's power higher performance

Publication details

Publisher

T-Systems International GmbH
Telekom Security - Cyber Defense Response and Testing
Bonner Talweg 100
53113 Bonn
Germany

Autor
T-Systems
23.12.2019

Inhaltsverzeichnis

1 Einleitung

Das IT-Dienstleistungszentrum (ITDZ) informierte das Berliner Kammergericht (KG) am 25.09.2019 über eine potentielle Information mit Schadsoftware innerhalb des Netzwerks des KG. Grund für die Benachrichtigung war die Kommunikation zu bekannten Command-and-Control (C2) Servern, welche dem ITDZ als IT-Provider des KG in den Logdaten der dort eingesetzten Proxy-Server auffiel. Als Reaktion wurde im Kammergericht eine Abschaltung der Internetkommunikation für das Kammergericht durchgeführt.
Aufgrund der hausinternen Untersuchung wurde ein Befall mit der Schadsoftware Emotet vermutet. Als Konsequenz beauftragte das KG die T-Systems mit der forensischen Untersuchung dieses Sicherheitsvorfalls. Die Beauftragung erfolgte am 01.10.2019.

Beteiligte Fachbereiche

Kammergericht
- Informationssicherheitsbeauftragter der o.G.
- Server-Administration

T-Systems
- Major Incident Management
- Forensik

Parallele Aktivitäten

McAfee
- hat die eingesetzte Software überprüft und aktualisiert

FA. DTS
- hat eine erste forensische Bewertung vorgenommen

LKA
- strafrechtliche Ermittlungen

1.1 Ziele der Forensischen Untersuchung

Das Ziel der forensischen Untersuchung wurde in einem Vor-Ort Termin beim Kammergericht in Berlin definiert. Die Zieldefinition wurde im Dokument „Ziele Forensik KG Sep/Okt 2019 vom 08.10.2019“ vom Kammergericht definiert. Das übergreifende Ziel der Untersuchung war die Ermittlung von Informationen zum Ausmaß des eingetreten Störfalls. Als zusätzliches Ziel wurde abgestimmt, dass konstruktive Hinweise für eine sichere IT-Architektur aufgezeigt werden sollten. Vier forensische Ziele sind klar definiert mit absteigender Priorität:

1. Welche Indizien/Beweise lassen sich finden, dass auf den Systemen des KG manipuliert wurde bzw. Fremdzugriffe stattfanden?
2. Lassen sich unautorisierte Maßnahmen finden?
3. Lassen sich Informationen zur Risikoabschätzung „betroffenes Gerät/System“ versus „Gerät/System ist Schadsoftwarefrei“ finden?
4. Wann und wo war der Ursprung des Sicherheitsvorfalls?

Aufgrund der Netzwerkstruktur des KG ließ sich nicht klar definieren welche Bereiche des Netzwerks betroffen/nicht betroffen sind. Zudem wäre es einem motivierten Angreifer möglich gewesen diese Netzstruktur auszunutzen, um fast jedes Gerät zu infizieren. Dadurch lässt sich der Bereich der Infektion nicht ohne eine vollumfängliche Analyse der gesamten Struktur des KG eingrenzen. Im Gespräch zum weiteren Vorgehen am 09.10.2019 wurde abgestimmt, dass eine solche zeit- und kostenintensive Untersuchung nicht durchgeführt wird. Stattdessen soll durch die Untersuchung eines hochwahrscheinlich infizierten Computers und des primären Domaincontrollers der Schaden abgeschätzt werden. Dadurch sollen Informationen gewonnen werden um die o. g. Ziele zu erreichen.

1.2 Datenerhebung

T-Systems Forensiker führten am 02.10.2019 eine Analyse vor Ort durch, um eine Ersteinschätzung der Lage vor Ort zu erheben. Hier wurden erste Indikatoren einer Malware Infektion gesammelt und gesichert. Zudem wurde durch das IT-Personal des KG Logfiles vom Web-Proxy bereitgestellt. Der Web-Proxy des KG Berlin wurde als Reaktion auf die Meldung des ITDZ so konfiguriert dass alle Client Anfragen in Logdateien aufgezeichnet werden.
Am 16.10.2019 ein Client und der primäre Domain Controller forensisch gesichert (Jeweils Arbeitsspeicher und Festplatten). Die Gesamtheit dieser Dateien bildet die Grundlage der forensischen Analyse.

2 Management Summary

Zur Untersuchung des IT-Sicherheitsvorfalls beim Kammergericht Berlin wurde eine forensische Untersuchung in zwei Stufen durchgeführt. Bei einer ersten Vor-Ort Untersuchung am 02.10.2019 wurde der Umfang des Incidents abgeschätzt. Die ersten Indikatoren deuteten auf einen schwerwiegenden Fall einer Emotet Infektion mit nicht abzuschätzenden Folgen für das Netzwerk, die Systeme und Daten des Kammergerichts hin. Diese Einschätzung beruhte auf drei Aspekten:

1. Auf Rechnern des Kammergerichts wurde an mehreren Stellen Malware gefunden, welche den typischen Kriterien der Schadsoftware Emotet entspricht.
2. Kurzfristig erhobene Logdateien eines Proxyservers zeigten Kommunikation zu Command and Control Servern, welche Emotet zuzuordnen sind.
3. Die IT-Infrastruktur des Kammergerichts ist nicht ausreichend vor Angriffen geschützt. Dem Angreifer ist es möglich gewesen mit einem Tunnel ins Netzwerk (bspw. durch einen infizierten Rechner) massiven Einfluss auf die Daten und Systeme des KG zu nehmen.

Basierend auf dieser Ersteinschätzung wurden in einem weiteren Vor-Ort Gespräch vom 09.10.2019 entschieden einen infizierten Computer und den primären Domaincontroller zu untersuchen. Diese Geräte wurden forensisch gesichert und im Forensiklabor der T-Systems untersucht.
Feststellung der Untersuchung ist, dass die initiale Infektion auf dem untersuchten Computer durch Emotet erfolgte. Der genaue Infektionsweg konnte anhand der gesicherten Systeme nicht identifiziert werden, da Logfiles nur teilweise vorlagen. Erfahrungsgemäß wird hierfür ein manipuliertes Word-Dokument mit aktivierten Makros verwendet. Emotet selbst lud auf dem untersuchten Computer die eigentliche Schadware TrickBot nach. TrickBot ist in der Lage beliebige Schadmodule auszuführen. Auf dem untersuchten Computer ließen sich drei Module identifizieren:

- Auf dem System gespeicherte Passwörter (insbesondere Browserpasswörter) werden extrahiert und an die Angreifer weitergeleitet.
- Dem Nutzer werden im Webbrowser Passwörter aktiv entlockt, insbesondere von Online-Banking Webseiten.
- Informationen über die Systeme werden dem Angreifer zugespielt.

Die besondere Schwere des Angriffs liegt in der fehlenden Netzwerksegmentierung des KG sowie lokale Administratorenaccounts der Nutzer. Auch erschwert das fehlende Logging am Proxyserver, welches erst nach Bekanntwerden des Incidents aktiviert wurde, die Aufklärung.

Eine Infektion des Active Directory kann nicht ausgeschlossen werden, wurde jedoch nicht nachgewiesen. Wir weisen jedoch ausdrücklich darauf hin, dass ein Angreifer höchstwahrscheinlich in der Lage gewesen ist, einen verborgenen Account anzulegen und den gesamten Datenbestand des KG zu exfiltrieren und zu manipulieren während gleichzeitig die Spuren verschleiert werden.

Aufgrund der Unwägbarkeiten der Infektion kann eine Kompromittierung der IT-Infrastruktur des KG nicht ausgeschlossen werden. Ein kompletter Neuaufbau der IT-Infrastruktur wird daher angeraten. Die Datenbestände (Exchange Server, Fileserver) müssen von Schadsoftware bereinigt werden bevor diese migriert werden können. Die Server selbst sollten ebenfalls neu aufgesetzt werden.

3 Technische Analyse A

In diesem Kapitel werden die gewonnen Erkenntnisse der Forensik beschrieben. Es wird auf die drei Schritte Voranalyse vor Ort, Analyse des Clients, und Analyse des primären Domaincontrollers eingegangen. Die Zeitzone für alle Datei-Zeitstempel in dieser Untersuchung ist UTC soweit nicht anders angegeben.

3.1 Voranalyse vor Ort

Während der ersten Analyse vor Ort am 02.10.2019 wurden vor allem Informationen gesichert um die Ausbreitung und die Verbreitungsmöglichkeiten der gefundenen Schadsoftware abzuschätzen. In Zusammenarbeit mit einem Consultant der Firma McAfee wurden Malware Samples untersucht und die Kommunikation mit dem Command and Control Server in den Logdaten der Proxy Server nachvollzogen. Bei der Analyse der Malwaresamples konnte bereits bekannte Schadsoftware festgestellt werden. Von Firma McAfee wurde versucht speziell auf die beim KG festgestellte Bedrohung zugeschnittene Signaturen zu erstellen.
Die Voranalyse hat eine tiefe Kompromittierung der Infrastruktur des KG aufgezeigt. Indizien wie fehlende Event Logs legen die Vermutung nahe das auch ein Zugriff durch Dritte von extern erfolgt ist und die Command and Control Verbindung aktiv zur Steuerung des Angriffs ausgenutzt wurde.

3.2 Forensische Sicherung der Daten vor Ort

Bei einem Vor-Ort Termin am 16.11.2019 wurden der Client mit der internen Bezeichnung und der primäre Domaincontroller gesichert. Es wurden jeweils der Hauptspeicher (RAM) sowie der Festplattenspeicher gesichert. Für eine forensische Sicherung wird eine Sicherung des Systems so durchgeführt wie das System vorgefunden wird um die vorgefundenen Zustände möglichst wenig zu verändern. Ist ein System zu Beginn der Sicherung bereits eingeschaltet wird daher zuerst der RAM gesichert um dann das System herunterzufahren und die Festplatten zu sichern. Ist das System heruntergefahren wird zuerst der Festplattenspeicher gesichert.
Der Client war beim Eintreffen vor Ort heruntergefahren; der Domaincontroller befand sich in Betrieb.

3.3 Analyse des Clients

Bei dem Betriebssystem des Clients handelt es sich um Windows 7 64bit mit Servicepack 1. Im Ersten Schritt der Analyse wird der Arbeitsspeicher auf laufende verdächtige Prozesse untersucht. Die Informationen aus dem Arbeitsspeicher werden dann mit den Dateien vom Image korreliert. Das Image enthält vier Partitionen, die Analysen fokussieren sich auf die Windows-Partition.
Alle Dateien des Rechners werden aufbereitet und sofern möglich die Zeitstempel extrahiert. Die resultierenden Daten werden zur Analyse eingespielt. Somit lässt sich eine Korrelation zwischen Systemereignissen wie Dateierstellung und Windows-Events ableiten.

3.3.1 Generelle Client Informationen

Für die nähere Untersuchung kamen durch den zeitlichen Rahmen der Infektion (letzter Login ab dem 01.01.2019) lediglich vier Nutzer in Frage.

1. Letzter Login am 25.09.2019 – 09:40:22
2. Letzter Login am 11.09.2019 – 13:45:21
3. Letzter Login am 16.06.2019 – 09:40:51
4. Letzter Login am 11.10.2019 – 08:52:45

3.3.2 Emotet: *tlblumber.exe*

Erkennung der Infektion im Arbeitsspeicher:
Bei einer Untersuchung aller Prozesse, welche eine Netzwerkverbindung aufbauen, fiel ein Prozess mit dem Namen *„tlblumber.exe"* auf, welcher auf allen lokalen Interfaces lauscht. Eine solche Datei wurde bereits in den Voranalysen als maliziös identifiziert.
Die von *tlblumber.exe* genutzten DLLs (Dynamic Link Library) sind Standard-Windows DLLs. Es handelt sich bei *tlblumber.exe* um eine gepackte Datei. Gepackte Dateien enthalten einen Entpackungsalgorithmus und einen obfuskierten Datenanteil. Beim Aufrufen wird zunächst die Payload der Schadware deobfuskiert und dann ausgeführt, um eine Analyse der Schadware zu erschweren.

Untersuchung der Schadware:
Die Datei *tlblumber.exe* selbst wurde aus dem Image extrahiert und in einer Sandbox gestartet. Durch die dynamische Analyse ergaben sich drei Findings:

1. Die Datei *C:\User\admin\AppData\Local\easywindow\easywindow.exe* wird erstellt
2. Kommunikation zu einem Comand and Control Server (C2 Server) findet statt
3. Bei *tlblumber.exe* handelt es sich um Emotet-Schadware

Die Datei *easywindows.exe* befindet sich zwar nicht auf dem vorliegenden Image, wurde aber auf anderen Systemen während der Voranalyse mehrfach gesichtet. Der Hash der in der VM-generierten *easywindow.exe* ist gleich der auf dem Image gefundenen *tlblumber.exe*, es handelt sich also um die gleiche Datei. Die C2 Server -Adresse wurde auch in den Voranalysen der Logdateien des Proxy Servers als C2-IP-Adresse identifiziert. Der Unterschied der Dateinamen und Speicherorte sind höchstwahrscheinlich Maßnahmen von Emotet, um die Analyse und Erkennung zu erschweren.

Das Verhalten von Emotet ist abhängig von einer in der *tlblumber.exe* integrierten Konfiguration. Über ein Skript ließ sich diese Konfiguration extrahieren. Die Konfiguration besteht aus OpenSSH-Credentials und zu kontaktierenden IP-Adressen. Auch hier findet sich die in der Sandbox kontaktierte IP-Adresse. Einige der kontaktierten IP-Adressen der Proxylogs aus der Voranalyse finden sich ebenfalls in der Konfiguration.

Spuren der Malware auf dem Image
Die Windows File-Informationen geben an, dass die Datei *tlblumber.exe* am 23.09.2019 um 12:49:32 erstellt wurde. Andere Dateiartefakte wie Windows Prefetch Dateien zeigen jedoch frühere Zeitpunkte an (*C:\Windows\Prefetch\TLBLUMBERB.EXE-472D4E9.pf*, erstellt am 20.09.2019 – 17:52:40). Daher wird der 20.09.2019 als Infektionszeitpunkt angenommen.

Die erste hier dokumentierte Ausführung von *tlblumber.exe* ist auf Freitag den 20.09.2019 um 13:30 datiert. Bis zum 23.09.2019 12:49 wurde die Datei 21-mal automatisiert gestartet.

Zwei Ausführungen von Dateien mit leicht anderem Namen (*tlblumbera.exe* und *tlblumberb.exe*) lassen sich auf Juli 2009 datieren. Der Grund für dieses Datum und weitere Informationen über diese Einträge sind nicht bekannt.

Erstinfektion mit *tlblumber.exe*
Aufgrund Häufung von zeitlichen Indikatoren wie die Erstellung der Prefetch Dateien und der Autostart-Einträge liegt der Infektionszeitpunkt **t0** für den untersuchten Client vermutlich am 20.09.2019 um 17:52:40. Der Zeitpunkt 20.09.2019 um 13:30 wird nicht als Infektionszeitpunkt angesehen, da hier keine weiteren zeitlichen Korrelationen existieren (Systemlogs, erstellte Dateien etc.) und von einem False-Positive ausgegangen wird.
Ausgeschlossen werden kann eine frühere Infektion jedoch nicht, da Zeitstempel überschrieben werden können und nur der Zeitstempel des jeweils letzten Events vorhanden ist.
t0 ist nur für den vorliegenden untersuchten Rechner gültig. Da Emotet sich typischerweise nicht wurmartig lateral ausbreitet kann aus **t0** keine allgemeingültige Aussage für andere Rechner gezogen werden. Laterales Movement durch nachgeladenen TrickBot von anderen infizierten Rechnern aus kann nicht ausgeschlossen werden.

3.3.3 TrickBot Infektion durch Emotet

Emotet selbst ist eine Schadware, welche den Weg in das Netzwerk für weitere Schadware anbietet. Typischerweise ist dies bei derzeitigen Infektionen eine Schadware mit dem Namen TrickBot TrickBot selbst bietet mehrere Module an, welche alle eigenständig arbeiten und Funktionen wie Ransomware-Erpressung, Kryptomining, oder andere Schadsoftware ausführen. Die genutzten Module werden oft in verschlüsselter Version als Konfigurationsdatei zusammen mit der TrickBot Malware heruntergeladen. TrickBot selbst entschlüsselt dann diese Konfigurationsdatei und agiert entsprechend der Anweisungen weiter.

Identifikation von TrickBot
Durch die Infektion mit *tlblumber.exe* ist eine vermutliche Erstinfektion am 20.09.2019 gegen 17:52:40 erkannt worden. Kurz darauf (17:53:17 bis 17:54:32) wurden mehrere weitere Dateien erstellt (Created Timestamp):

- \ProgramData\JrxZRaiaq1wQaciz2B.exe
- \Windows\Prefetch\TLBLUMBERB.EXE-76BCB4CB.pf
- \ProgramData\სახელმწიფო.exe
- \Windows\System32\config\systemprofile\AppData\Roaming\iCloud\სახელმწიფო.exe
- \Windows\System32\config\systemprofile\AppData\Roaming\iCloud\McTrayPluginStateHistory.txt
- \Windows\Prefetch\სახელმწიფო.EXE-BDB1E741.pf

Die Dateien *JrxZRaiaq1wQaciz2B.exe* und სახელმწიფო.exe sind unabhängig von ihrem Speicherort auf Basis ihrer Hashsumme identisch. Sie werden als TrickBot-Malware eingestuft.

Untersuchung von TrickBot

Im Windows Tasklplaner fand sich ein Task welcher auf die Datei *\Windows\System32\config\systemprofile\AppData\Roaming\iCloud\სახელმძღვ.exe* verweist und als Startzeit den 20.09.2019 um 19:54:25 angibt (UTC+2). Die Datei für den Taskplaner befand sich unter *C:\Windows\System32\Tasks\iCloud Free Disk*. Somit wurde das Starten der Schadware nach einem Reboot garantiert.
Die Datei *McTrayPluginStateHistory.txt* konnte zu einer XML-Datei entschlüsselt werden. In der entschlüsselten Konfigurationsdatei sind mehrere C2 Server-Adressen sowie die von TrickBot auszuführenden Module aufgelistet:

- module name="systeminfo" ctl="GetSystemInfo"
- module name="injectDll"
- module name="pwgrab"

Das Modul *systeminfo* liest Informationen wie das Betriebssystems des infizierten Rechners aus und leitet diese Informationen an den C2 Server weiter. Das Modul *injectDll* versucht login-Daten für Banken über Pop-ups abzugreifen und an den C2 Server zu senden. Das Modul *pwgrab* untersucht lokal hinterlegte Passwortdatenbanken für Browser und einige Softwareapplikationen und sendet diese an den C2 Server. Auch ist ein Identifier für die TrickBot Kampagne der Konfigurationsdatei beigelegt (*<gtag>mor5</gtag>*).

3.3.4 Infektionsweg

Der Infektionsweg auf dem Client konnte nicht nachvollzogen werden. Eine Verbreitung von Emotet ohne Office-Dokumente ist nicht geläufig. Daher ist auch in diesem Fall von einer derartigen Infektion auszugehen. In der Regel wird ein Emotet-Office-Dokument mit Makros als Anhang einer Email übermittelt. Wichtig für die Infektion ist jedoch nur das Ausführen des Dokuments und das Aktivieren der Makros (standardmäßig in Office deaktiviert).
Die auf dem Rechner gespeicherten Emails aus dem Jahr 2019 sind alle einem User zugeordnet. Die letzte empfangene Mail ist auf den 11.09.2019 um 12:20:43 datiert. In den Mails ließen sich keine mit Makros versehenen Office-Dokumente und mit Emotet infizierten Anhänge identifizieren.

Eine Suche auf dem Dateisystem nach Office-Dokumenten verlief ebenfalls ohne Befund. Das jüngste Dokument auf dem System ist ein autogeneriertes Outlookdokument vom 16.05.2019 um 11:05:06.

Möglich ist das Aufrufen einer Webmail Website und das Öffnen des manipulierten Office-Dokuments über den Browser. Daher wurde die Internet-Historie untersucht. Es finden sich auch hier keine Indizien für eine der Infektion zuzuordnenden Website oder den Download einer maliziösen Datei.
Die letzten Zugriffe fanden am 11.10.2019, also deutlich nach der Infektion, durch den Internet Explorer statt.
Zwischen dem 23.09.2019 um 04:57:49 und dem 25.09.2019 ließen sich Zugriffe über den Internet Explorer nachweisen.
Auch sind Zugriffe vom 11.09.2019 zwischen 11:08:22 und 12:38:02 auf Dateien festzustellen. Die Namen der Dateien wurden auch als Dateinamen in Email-Anhängen aus Mitte September entdeckt und als unbedenklich eingestuft.

Ein weiterer denkbarer Infektionsweg ist ein USB-Datenträger welcher die maliziöse Datei enthält. Hierbei fallen zwei Datenträger in einen denkbaren Zeitraum:

- 11.10.2019 – 08:47:28 Kingston Data Traveler
- 11.09.2019 – 11:07:40 Kingston Data Traveler

Eine Infektion über einen USB-Stick kann weder ausgeschlossen, noch nachgewiesen werden. Der genaue Infektionsweg kann nicht bestimmt werden. Eine Infektion über den Fileserver ist nicht auszuschließen.

3.4 Analyse des primären Domaincontrollers

Als zentrales Element der KG Netzinfrastruktur ist der (primäre) Domaincontroller (DC) von hoher Priorität für einen Angreifer. Indikationen für eine Infektion des DC würden weitreichende Manipulationen des Angreifers nachweisen und stellen das Worst-Case Szenario dar.
Der Server basiert auf Windows Server 2008R2x64 mit ServicePack1. Aus der Registry1 ließ sich ermitteln, dass der Server am 05. April 2015 in Betrieb genommen wurde. Es wurden keine Auffälligkeiten in den Shutdown- und Bootvorgängen gefunden. Eine virtuelle Maschine liegt vor und wird in der Analyse zum Abgleich zwischen den beiden Servern genutzt, ist jedoch nicht im Fokus der Forensik.
Bei der Analyse werden die gleichen grundlegenden Tools und Methoden genutzt, welche auch beim Client verwendet werden.

3.4.1 Untersuchung der Registry

Alle im Arbeitsspeicher präsenten Prozesse sind unauffällig. Die vorgefundenen Netzwerkverbindungen entsprechen den Funktionen des Servers (LDAP, DNS). Es konnten keine versteckten Prozesse gefunden werden.

Die Untersuchung gängiger Persistenzmechanismen für Schadware wie Einträge in Autostart-Registry Schlüsseln oder Tasks fand keine maliziösen Aktivitäten.

Dem Registry Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR* sind zwei angeschlossene USB-Datenträger zu entnehmen, welche im Jahr 2019 angeschlossen wurden. Ein Datenträger ist der für die RAM-Sicherung genutzte Storejet Transcend was über Seriennummer und Datum bestätigt wurde. Bei dem anderen Gerät handelt es sich um ein USB-Gerät der Firma Patriot Memory, welches am 10.10.2019 um 06:46:27 angeschlossen wurde. Ob es sich hierbei um eine legitime Verbindung oder die Quelle der Infektion handelt lässt sich durch die vorliegende Datenbasis nicht klären.

3.4.2 Untersuchung der Windows Event Logs

Informationen über Windows Server finden sich in den Windows Event Logs, welche sich in diversen .evtx Dateien auf dem Windows Server befinden. Insbesondere die sicherheitskritischen Eventlogs aus der Datei *\Windows\System32\winevt\Logs\Security.evtx* wurden untersucht. Für Eventlogs ist ein Größenlimit konfigurierbar. Ist das Limit erreicht werden frühere Daten aus den Logs gelöscht um Platz für neuere Daten zu schaffen. Die Sicherheitseventlogs reichen lediglich vom 16.10.2019 um 13:10:06 bis zum 14.10.2019 um 13:23:37 zurück. Die Dateigröße von 128MB deutet auf das Erreichen der maximalen Logfilegröße hin. Dadurch können keine Aussagen über Loginaktivitäten durch einen etwaigen Angreifer vor dem 14.10.2019 getroffen werden. Dies ist insbesondere mit Hinblick auf den Infektionszeitraum um den 20.09.2019 problematisch. Die Konfiguration der Logfilegröße sollte so abgeändert werden, dass mehrere Monate betrachtet werden können.

Die vorhandenen Logdaten zeigen Logins mit Eventcode 4624 und Logon Type 2 was für manuelle interaktive Logins (Remote und Local) steht.

Am 14.10.2019 um 15:02:27 wurde ein gescheiterter Loginversuch dokumentiert.
Es wurden zudem mehrere gescheiterte Loginversuche vom 16.10.2019 um 09:43:04 bis zum 16.10.2019 bis 09:57:03 beobachtet, die während der forensischen Sicherung entstanden sind und damit als unbedenklich eingestuft werden.
Zudem wurde ein einzelner gescheiterter Loginversuch am 16.10.2019 um 12:25:21 dokumentiert welcher ebenfalls der Sicherung zuzuordnen ist. Die Zeiten sind in GMT+0 angegeben.

Logon Type 3 beschreibt Logins durch automatisierte Dienste wie z. B. Kerberos oder Fileserver-Zugriffe. Hier sind zwischen dem 14.10.2019 13:24:06 und dem 16.10.2019 13:09:03 33.613 Zugriffe dokumentiert, welche aufgrund der Serverfunktion als Domaincontroller zu erwarten sind.

Zwischen dem 14.10.2019 13:42:36 und dem 16.10.2019 13:05:03 wurden 30 Logins mit Logon Type 5 dokumentiert. Diese werden durch die Aktivierung von System-Services ausgelöst.

Auch unter Logon Type 7, welcher Unlocks aus dem gesperrten Zustand beschreibt, finden sich nur legitime Logon Events aus dem zeitlichen Bereich der forensischen Datensicherung.

Es finden sich zwei Remote Logins (Logon Type 10) am 14.10.2019 um 14:24:15 und 15:03:20. Es ist zu klären ob es sich hierbei um legitime Logins handelt.

Weitere Event-IDs wie unter anderem die IDs 4724 (Zurücksetzen eines Passworts), 4735 (Lokale Gruppe verändert), 4738 (Passwort geändert) oder 7045 (Ein Service wurde installiert) konnten durch das Logfile-Limit nicht in den Eventlogs gefunden werden.

3.4.3 Untersuchung des Active Directory

Kerndatei des Active Directory ist die *ntds.dit*. In dem vorliegenden Image des heruntergefahrenen Domain Controllers ist diese Datei auf der RAID5 Datenpartition vorhanden (unter *\NTDS\ntds.dit)* aber leer. Bei einer Überprüfung durch das KG am 29.10.2019 ergab sich, dass die Datei auf dem Domaincontroller (in Betrieb) mit einer Größe von 1,02GB wie erwartet vorliegt. Die Ursache dieser Diskrepanz ist nicht bekannt.
Um trotzdem Manipulationen der Domäne erkennen zu können wird die *ntds.dit* Datei des sekundären Domaincontrollers extrahiert und untersucht. Zwischen den beiden Domaincontrollern bestand eine Synchronisierung auf Netzwerkebene. Die Netzwerkverbindung zwischen den

Domaincontrollern wurde am 29.09.2019 aufgrund der Emotet Infektionen unterbrochen und nicht wieder in Betrieb genommen.
Die verdächtigen Veränderungen an der Active Directory Struktur basierend auf den Ergebnissen der *ntds.dit* sollten durch die Adminstratoren des KG untersucht werden (legitim oder nicht legitim).

3.5 Fazit

Der Befall der IT-Infrastruktur des KG Berlin ist schwerwiegend. Es konnten klare Beweise für eine Infektion mit bekannter Malware festgestellt werden. Durch Untersuchung eines Clients ist eine Infektion ab spätestens 20.09.2019 um 17:52 nachgewiesen.
Die Erkennung der auf den Systemen gefundenen Malware Varianten durch die Endpoint Protection Lösung von McAfee war zum Zeitpunkt der Infektion nicht gegeben. Die konkreten Fragestellungen der Untersuchung sind im Folgenden noch einmal konkret aufgeführt.

1. Welche Indizien/Beweise lassen sich finden, dass auf den Systemen des KG manipuliert wurde bzw. Fremdzugriffe stattfanden?

   Klare Infektion durch Trickbot und Emotet Malware vorgefunden, AD Zugriffe nicht lückenlos rekonstruierbar, da die vorhandenen Logdateien nicht ausreichend waren.

2. Lassen sich unautorisierte Maßnahmen finden?

   Ja, Die Module von Trickbot sind klar auf Datenabfluss ausgerichtet. Eine Verschlüsselung oder Manipulation von Dateien auf den Geräten konnte nicht nachgewiesen werden.

3. Lassen sich Informationen zur Risikoabschätzung „betroffenes Gerät/System“ versus „Gerät/System ist schadsoftwarefrei“ finden?

   Es gibt klare Indicators of Compromise, diese sind aber sicherlich nicht konklusiv. Eine individuelle Bereinigung ggf. durch eine Sandboxlösung wie die FireEye FX-Serie muss erfolgen.

4. Wann und wo war der Ursprung des Sicherheitsvorfalls?

   Der Ursprung des Sicherheitsvorfalls ist weiterhin unbekannt. Aufgrund der Struktur von Emotet und dem üblichen Verhalten ist von E-Mails mit bösartigen Makros in Worddokumenten auszugehen. Durch die IT- Infrastrukur (keine Netzwerksegmentierung, keine Filterung am Gateway, keine Proxy Logdaten, lokale Administratoren, mangelnde AD Logs) wurde aus einem Standardvorfall ein massiver Incident.
   Zusätzlich konnten klare Mängel bei der Leistungsfähigkeit bzw. Aktualität der Endpoint Protection Lösung von McAfee festgestellt werden. Diese hat Malware die zum Zeitpunkt der Infektion bereits bekannt war nicht erkannt.

3.6 Empfehlungen:

Die T-Systems empfiehlt umfangreiches Logging auf allen Servern und Arbeitsplatzsystemen, um Vorfälle besser nachvollziehbar zu machen. Eine klare Netzwerksegmentierung sowie ein fein gegliedertes Berechtigungskonzept können den Umfang von Incidents deutlich verringern.
Es wird empfohlen die gesamte Windows Domäne neu aufzusetzen, auch um eventuelle Altlasten nicht zu übernehmen. Das KG Berlin kann die aktuelle Situation nutzen um ein leistungsfähiges und sicheres neues Netzwerk zu konstruieren und den Schaden bei zukünftigen Vorfällen stark zu begrenzen.