

Rahmenplan zur wöchentlichen CSCC-Telefonkonferenz

Termin	Inhalt	Verantwortlich
bis Do 12:00	Meldung von Sicherheitsvorfällen der vorigen Woche an TÜV TRUST IT ¹	CSCC-Mitglieder
bis Do 18:00	Aufbereitung und Konsolidierung der gemeldeten Sicherheitsvorfälle	TÜV TRUST IT
bis Fr 09:30	Versand der Einwahldaten und ggf. Hintergrundinformationen	TÜV TRUST IT
Fr 10:00–12:00	CSCC-Telefonkonferenz Einwahl:+49 69 2108 69 700 Teilnehmercode: (wird am Vormittag verschickt)	alle
Fr 12:00–14:00	Möglichkeit für individuelle telefonische Beratung bzw. Nachfragen	TÜV TRUST IT
Anschließend (Fr. oder Mo.)	Zusendung des Berichts und des Protokolls an die CSCC-Mitglieder	TÜV TRUST IT

¹ S/MIME- oder GnuPG-verschlüsselt an csc@it-tuv.com
S/MIME-Fingerprint: 5163c0a1 b037025e 26ed1d45 62edf557 326ee50f
GnuPG-KeyID: 759B ABB7 21E6 A0F5 5E2F FDC0 0D09 E091 2F9E 3E57

Agenda zur wöchentlichen CSCC-Telefonkonferenz

Einwahl:..... +49 69 2108 69 700

Admincode: [über das Konferenzportal erstellt und bis 09:30h versandt]

Teilnehmercode: [über das Konferenzportal erstellt und bis 09:30h versandt]

TOP	Inhalt	Verantwortlich
0	<u>Begrüßung, Vollzähligkeit</u> ggf. Vorstellung neuer Teilnehmer	TÜV TRUST IT
1	<u>Offene Punkte der Vorwoche</u> Sofern aus vergangenen Telefonkonferenzen noch offene Punkte zur Klärung vorliegen, werden diese hier besprochen.	TÜV TRUST IT
2	<u>TÜV Case der Woche</u> Eine aktuelle Entwicklung aus dem Umfeld der IT-Sicherheit wird vorgestellt, Hintergründe und Zusammenhänge erläutert und Auswirkungen und mögliche Mitigationsstrategien gegeben.	TÜV TRUST IT
3	<u>Aktuelle Sicherheitslage</u> Die wesentlichen, seit der letzten Telefonkonferenz aufgetretenen externen Ereignisse mit Bezug zur IT-Sicherheitslage werden kurz vorgestellt, im Hinblick auf ihre Relevanz bewertet und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen.	TÜV TRUST IT
4	<u>Auswertung gemeldeter Sicherheitsvorfälle</u> Die in der vergangenen Woche aufgetretenen Sicherheitsvorfälle werden in anonymisierter und konsolidierter Form vorgestellt und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen	TÜV TRUST IT sowie ggf. weitere Experten
5	<u>Diskussion und Rückfragen</u> Beantwortung bzw. Sammlung weiterer Rückfragen	alle

Im Nachgang zur wöchentlichen Telefonkonferenz besteht die Möglichkeit, individuelle Rücksprache zu Sicherheitsthemen in individuellen Telefonterminen wahrzunehmen.

CSCC Case der Woche


2017-05-23: Angriffskampagne „Operation Cloud Hopper“

Titel Angriffskampagne „Operation Cloud Hopper“	Risiko ■■■■□□
Betroffene Systeme:	./
Sachstand:	<p>Das Bundesamt für Verfassungsschutz (BfV) warnt in seinem aktuellen Cyber-Brief vor einer Angriffskampagne der chinesischen Gruppierung APT10, auch bekannt als „Menupass Team“ oder „Stone Panda“.[1] Die Kampagne mit dem Namen „Operation Cloud Hopper“ richtet sich gezielt gegen Managed Service Provider bzw. Cloud-Dienste. APT10 ist seit ca. 2009 aktiv und fokussierte sich anfangs auf japanische und US-amerikanische Ziele. Seit Ende 2016 sollen auch Unternehmen in Europa Angriffen ausgesetzt sein, das Interesse der Gruppierung liegt primär bei folgenden Branchen:</p> <ul style="list-style-type: none"> • Energie • Transport/Automobil • Rohstoffe/Mineralien • Chemie • Gesundheit • Telekommunikation • Luft- und Raumfahrt <p>Angriffe erfolgen meistens durch gezielte Spear-Phishing Mails mit manipulierten Word-Dokumenten. Zu dem „Arsenal“ von APT10 zählt unter anderem die Schadsoftware „ChChes“, die selbst wenige Funktionen mitbringt, bei Bedarf aber Module über Command-&-Control Server herunterladen kann.</p>
Bewertung:	<p>APTs stellen unverändert eine der höchsten Bedrohungen für Unternehmen dar, da sie sowohl über fachliche als auch finanzielle Ressourcen zur Durchführung ihrer Kampagnen verfügen. Bisher stand APT10 weniger im Fokus von europäischen Unternehmen, weshalb zurzeit vergleichsweise wenig Informationen aus europäischen Quellen verfügbar sind. Da APT10 aber bereits länger bekannt und aktiv ist, haben andere Institutionen tiefergehende Analysen durchgeführt, beispielsweise das japanische CERT zur Schadsoftware ChChes.[2]</p>
Empfehlung:	<p>Der Cyber-Brief des BfV enthält eine Liste mit Domains und IP-Adressen (<i>Indicators of Compromise</i>). In den Netzwerk-Logs kann gezielt nach Verbindungen zu diesen Endpunkten gesucht werden. Da Domains und IP-Adressen dynamisch und kurzlebig sein können, sind aufgezeichnete Verbindungen nicht zwingend ein Beweis für einen erfolgreichen Angriff. In diesem Fall sind weitere, bedarfsabhängige Maßnahmen einzuleiten.</p>
Quellen:	<p>[1] BfV Cyber-Brief Nr. 02/2017 [2] ChChes - Malware that Communicates with C&C Servers Using Cookie Headers</p>
Point of Contact:	<p>André Zingsheim, andre.zingsheim@tuv-austria.com, 0221/969789-83</p>

2017-05-22: „Cloak & Dagger“-Angriff gegen Android

Titel		Risiko
„Cloak & Dagger“-Angriff gegen Android		■■■□□
Betroffene Systeme:	Android 5.1.1, 6.0.1, 7.1.2 (bestätigt) Android < 5.1.1 (vermutet)	
Sachstand:	<p>Sicherheitsforscher haben einen Angriff auf Android-Geräte demonstriert, welcher unter anderem die Installation von Dritt-Apps oder das Ausspionieren sensibler Informationen wie Passwörter und PINs ermöglicht.[1] Der Angriff mit den Namen „Cloak & Dagger“ basiert auf der Kombination der zwei Android-Berechtigungen „SYSTEM_ALERT_WINDOWS“ und „BIND_ACCESSIBILITY_SERVICE“ und realisiert im Wesentlichen einen Clickjacking-Angriff, d. h. der Anwender befindet sich in dem Glauben, mit auf dem Display befindlichen Element (Buttons, Textfelder) zu interagieren. In der Realität liegt jedoch über diesen Elementen eine weiteres, für den Benutzer unsichtbares und vom Angreifer kontrolliertes User-Interface.</p> <p>Der Angriff wurde unter den Android-Versionen 5.1.1, 6.0.1 und 7.1.2 verifiziert, welche zusammen ca. 70 Prozent des Android-Marktanteils ausmachen. Die Sicherheitsforscher vermuten stark, dass auch vorherige Versionen betroffen sind. Bei einem Test unter 20 Benutzern war die Installation einer Dritt-App im sogenannten „God-Mode“ nicht ersichtlich, sodass ein erfolgreicher Angriff mit großer Wahrscheinlichkeit für den Benutzer völlig transparent geschieht.</p>	
Bewertung:	Die Forscher stehen seit August 2016 mit Google im Kontakt. Seitdem vertreten die beiden Parteien unterschiedliche Meinungen (Sicherheit-slücke vs. Feature), sodass keine konkreten Updates zu erwarten sind, wenngleich Google für das nächste Android Release („Android O“), welches im 3. Quartal 2017 erscheint, Besserung gelobt.	
Empfehlung:	Android-Benutzer können praktisch kaum Maßnahmen ergreifen, da die beiden Berechtigungen automatisch gewährt werden, sobald der Benutzer eine App aus dem PlayStore installiert. Die beste Maßnahme bestehe daher ausschließlich in der Installation von Apps aus dem PlayStore, da Google den Store gezielt nach der Kombination der beiden Berechtigungen durchsuchen wolle. Allerdings ist es den Forschern gelungen, eine App mit exakt diesen beiden Berechtigungen im PlayStore zu veröffentlichen, in dem diese nach wie vor verfügbar ist.	
Quellen:	[1] Cloak & Dagger	
Point of Contact:	André Zingsheim, andre.zingsheim@tuv-austria.com , 0221/969789-83	

2017-05-25: Angriffe mittels präparierter LNK-Dateien

Titel Angriffe mittels präparierter LNK-Dateien	Risiko 
Betroffene Systeme:	./
Sachstand:	<p>TrendMicro hat seit Beginn des Jahres einen signifikanten Anstieg bei Angriffen, die mittels präparierter LNK-Dateien initiiert werden, registriert.[1] LNK-Dateien, unter Windows auch bekannt als Shortcuts bzw. Verknüpfungen, verweisen auf andere Programme, die dann wiederum weitere Aktionen ausführen.</p> <p>In einem kürzlich registrierten Angriff verwies eine Verknüpfung auf das Programm MSHTA.exe (ein Programm zur Anzeige von HTML-Dateien), in dem JavaScript ausgeführt wird, welches wiederum PowerShell-Skripte nachlädt und ausführt.</p> <p>Eine LNK-Datei kann durch mehrere Parameter flexibel gestaltet werden.</p>
Bewertung:	<p>Angriffe über LNK-Dateien sind grundsätzlich nicht neu, sie haben in der Vergangenheit aber vergleichsweise wenig Aufmerksamkeit erzeugt, unter anderem da Angriffe durch manipulierte Office Makros in vielen Fällen effektiver waren. Die Verwendung von Verknüpfungen als Ausgangspunkt für einen Angriff in der Angriffskampagne „Operation Cloud Hopper“ belegen, dass die Dateien sogar zu den Angriffstechniken der APTs zählen.</p>
Empfehlung:	<p>LNK-Dateien können als erste Instanz am Mailgateway blockiert werden. Sofern die Dateien allerdings in Office-Dokumente eingebettet werden, wird die Erkennung und Filterung erschwert.</p> <p>Da der Angriff letztendlich in vielen Fällen in der Ausführung von PowerShell-Skripten mündet, kann die Aktivierung von PowerShell-Logging ein weiteres Hilfsmittel bei der Erkennung schädlicher Aktivitäten sein.</p> <p>Eine Sensibilisierung des Benutzers zum Umgang mit Verknüpfungen scheint ein eher ungeeigneteres Mittel zu sein.</p>
Quellen:	<p>[1] A Rising Trend: How Attacks are Using LNK Files to Download Malware</p>
Point of Contact:	<p>André Zingsheim, andre.zingsheim@tuv-austria.com, 0221/969789-83</p>