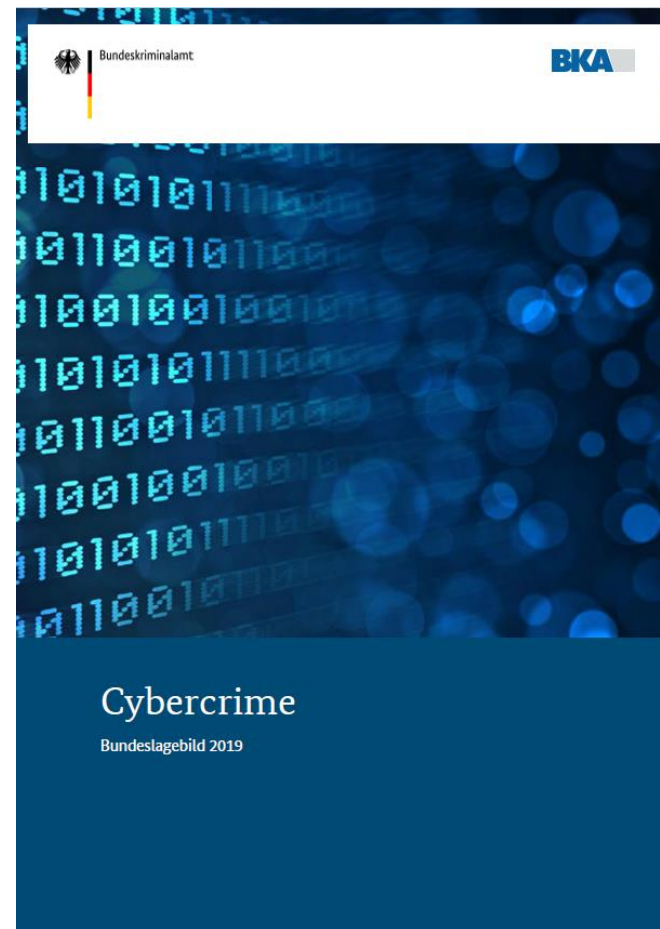
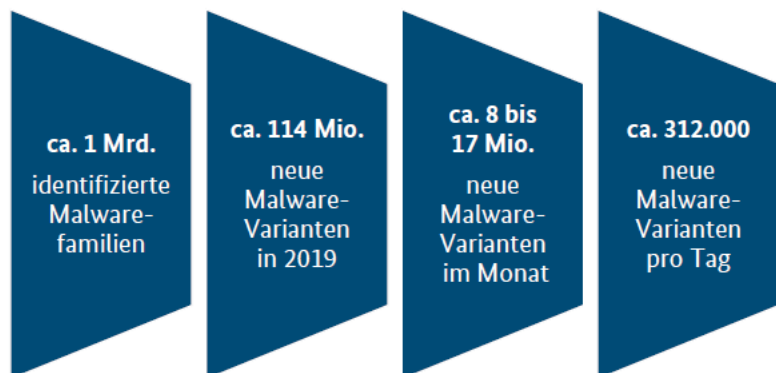


Cybercrime wird immer professioneller



Cyberkriminelle müssen keine Informatiker sein – Crime as a service

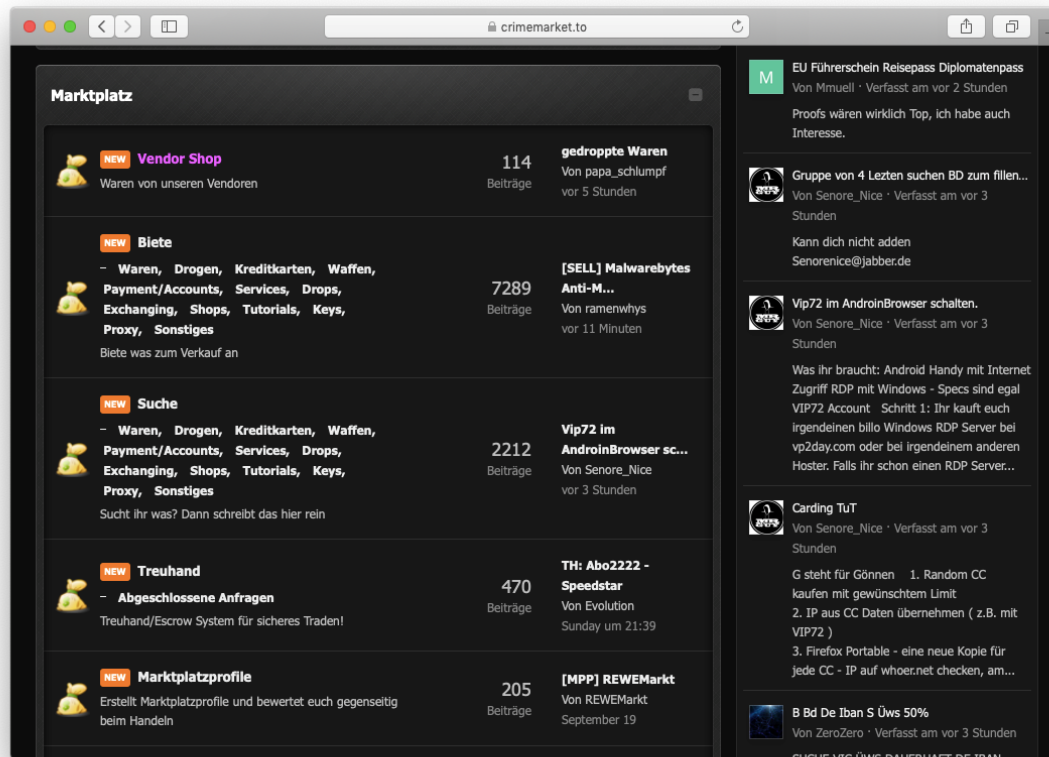
The screenshot shows the website **crimemarket.to** with the tagline "UNDERGROUND ECONOMY". The interface includes a search bar, navigation tabs (Forums, Aktivität, Chatbox, Eigene Themen, Treuhand), and a user profile for "florianschneider". A green notification banner states: "Kostenlos Treuhand nutzen für sichere Trades. Bei Problemen mit Usern und Betrug Report eröffnen. Spendenwallet: 12KeMsqyx5KA755VoBjHhNiDy4p4koxLnc (Info Thread)".

The main content area features a large advertisement for **BKA.CARDS** with the text "KREDITKARTEN" and "DER-DEUTSCHE.TO". Below this is an advertisement for "UMGEFÜLLT 50ML BY CRIMETIME1" featuring various perfume bottles and logos for Bitcoin and PaysafeCard. At the bottom of the ad, it says "48H LIEFERUNG".

On the right side, there is a Bitcoin price widget showing a price of €9,779.11 and a 24h change of +1.07%. Below that is a "Posts" section with two entries:

- Biete 1x Vivid mit Visa Debit Card Suche 3...** Von Gruengras · Verfasst am vor 1 Minute push
- Biete Faked PS ohne GC und SIM Suche 1...** Von Gruengras · Verfasst am vor 1 Minute push

Cyberkriminelle müssen keine Informatiker sein – Crime as a service



Cyberkriminelle müssen keine Informatiker sein – Dienstleistung für Erpressung/Computersabotage

- DDoS Service by f0x - 400k R/S - 150Gbps -



The screenshot shows a forum post by a user named 'f0x'. The user's profile picture is a silhouette of a person wearing a hat and sunglasses. The post title is '- DDoS Service by f0x - 400k R/S - 150Gbps -' and it was posted on '16. Mai 2017' with '+1' upvotes. The post content offers DDoS services for websites, game servers, and voice servers. A price list is provided: 'Nicht geschützter Server / Webseite - 5€ / stündlich', 'Schlecht geschützter Server / Webseite - 10€ / stündlich', 'Medium geschützter Server / Webseite - 25€ / stündlich', and 'Gut geschützter Server / Webseite - 75€ / stündlich'. The post also states that the attacker will judge the website's security level and that no stressers or booters are used. It concludes with a note that screenshots of attacked websites are available and that a test hit can be arranged upon interest.

f0x

- DDoS Service by f0x - 400k R/S - 150Gbps -
16. Mai 2017 +1

Biete euch meine **DDoS** Services an.
Unter anderem für Webseiten / Game und Voice Server.

Preisliste:

- Nicht geschützter Server / Webseite - 5€ / stündlich
- Schlecht geschützter Server / Webseite - 10€ / stündlich
- Medium geschützter Server / Webseite - 25€ / stündlich
- Gut geschützter Server / Webseite - 75€ / stündlich

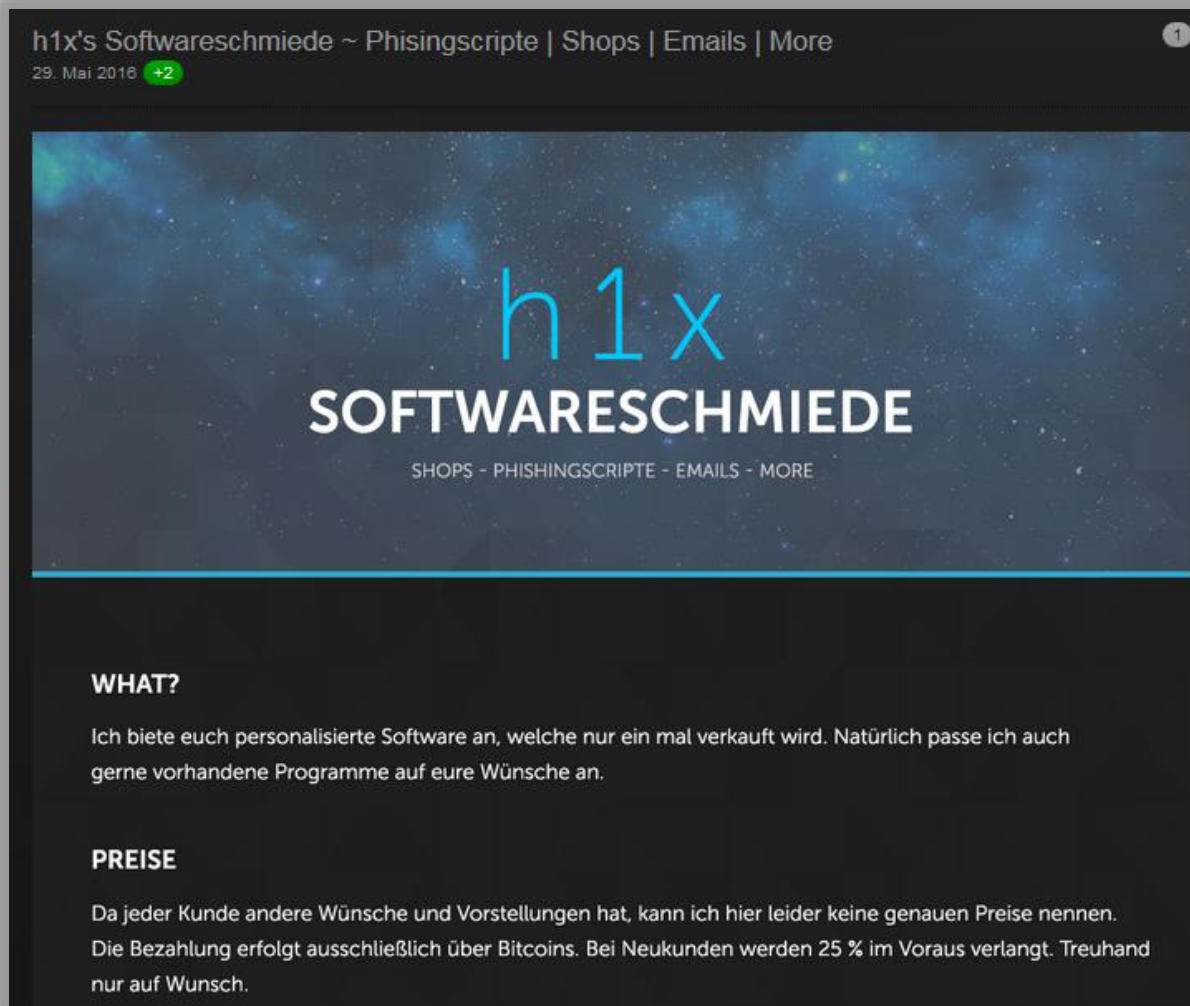
Die einstufung der Webseite die ihr attackieren wollt beurteile ich.
Es wird kein stresser / booter für diese Attacken benutzt.

Hier einige Screenshots von Webseiten die von mir attackiert wurden,
Selbstverständlich kann ein Test-hit bei Interesse gemacht werden.

Pre-Member

Erhaltene Likes:	1
Punkte:	14
Beiträge:	1
Themen:	

Handel mit Schadsoftware



h1x's Softwareschmiede ~ Phisingscripte | Shops | Emails | More

29. Mai 2016 +2

h1x

SOFTWARESCHMIEDE

SHOPS - PHISHINGSCRIPTS - EMAILS - MORE

WHAT?

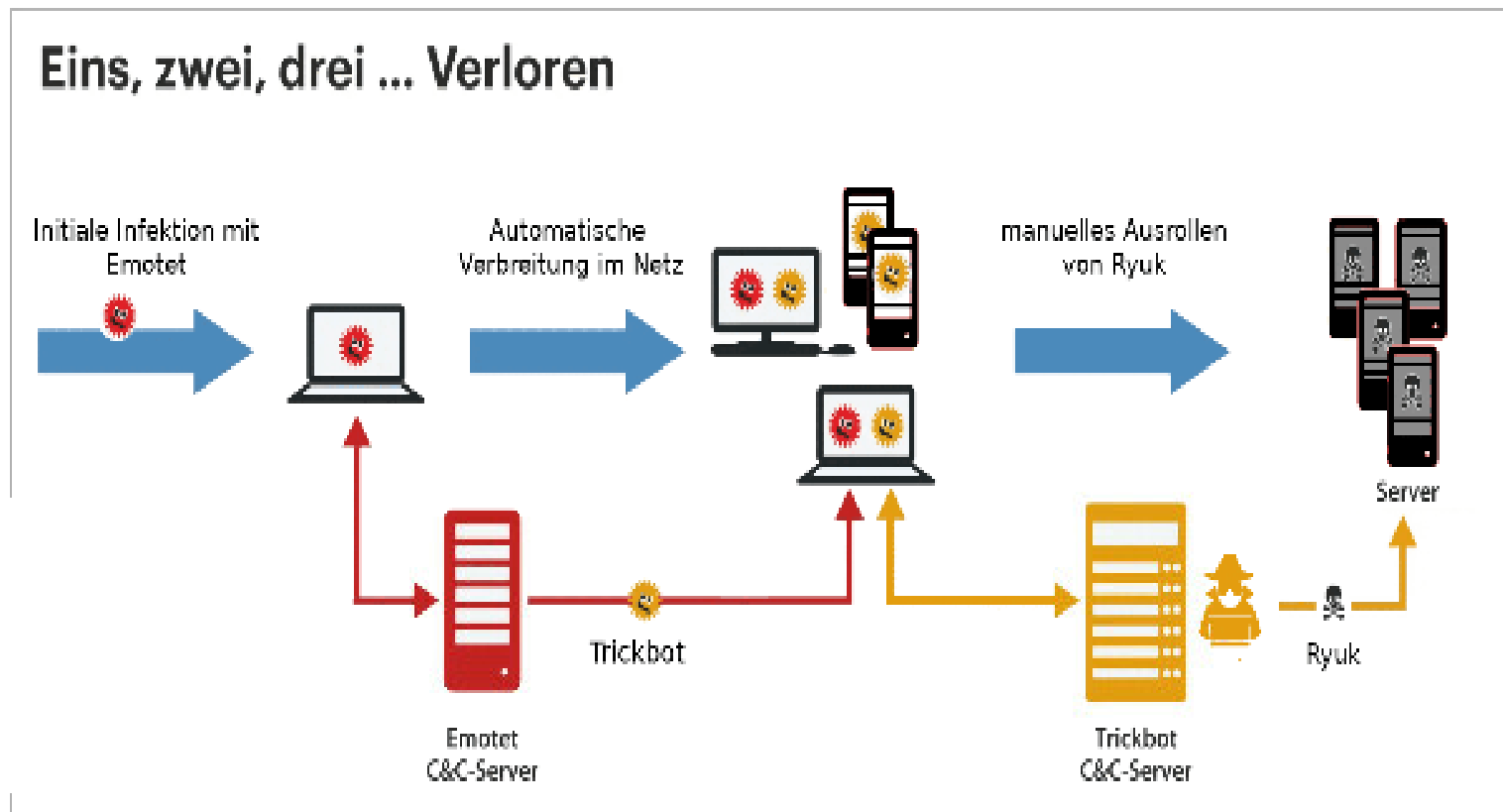
Ich biete euch personalisierte Software an, welche nur ein mal verkauft wird. Natürlich passe ich auch gerne vorhandene Programme auf eure Wünsche an.

PREISE

Da jeder Kunde andere Wünsche und Vorstellungen hat, kann ich hier leider keine genauen Preise nennen. Die Bezahlung erfolgt ausschließlich über Bitcoins. Bei Neukunden werden 25 % im Voraus verlangt. Treuhand nur auf Wunsch.



Gang der Infektion



Der bösartige Dreischritt: Infektion mit Emotet, Sekundärinfektion mit Trickbot und dann das manuelle Ausrollen von Ryuk, das wichtige Daten verschlüsselt. (Bild: Heise)

Wer ist in Deutschland betroffen?

- Gerichte
- Bundesbehörden
- Stadtverwaltungen
- Uni-Kliniken
- Arztpraxen
- Universitäten
- Schulen
- mittelständische Unternehmen

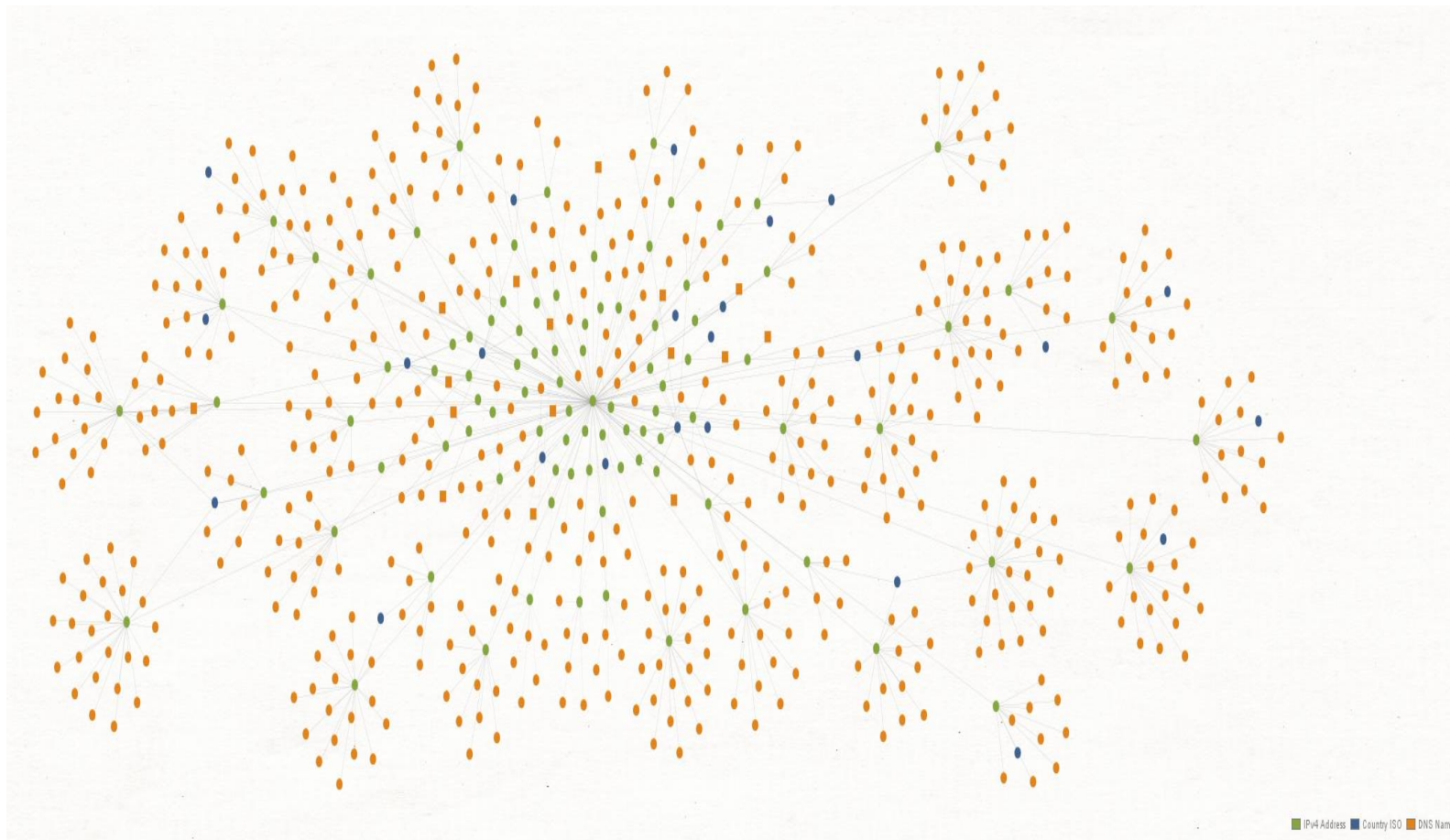
Der Beginn unseres Verfahrens

- Hinweis beim BKA im Rahmen der phänomenologischen Auswertung auf Emotet
- Hinweis auf Adresse eines in Brasilien gehosteten Servers, von dem aus Schadsoftware im Zusammenhang mit Emotet nachgeladen wurde und dessen Logfiles frei einsehbar waren
- in diesen Logfiles konnte ein für die technische Infrastruktur der Emotet-Schadsoftware relevantes System in Deutschland festgestellt werden

Der Beginn unseres Verfahrens

- Server-Standort in DE
- Übernahme der Ermittlungen durch die ZIT und Überwachung des Servers
- „Ursprung-Server“ letztlich Sackgasse, aber die Analyse der Schadsoftware durch die Ermittler des BKA ergab letztlich werthaltige Ansätze, viele Server-TKÜen sollten folgen

Die Emotet-Infrastruktur



Internationale Partner Strafverfolgungsbehörden aus 7 Ländern:

Niederlande: *Politie und Landelijk Parket*

USA: *Federal Bureau of Investigation, U.S. Department of Justice und
US Attorney's Office for the Middle District of North Carolina*

Kanada: *Royal Canadian Mounted Police*

UK: *National Crime Agency und Crown Prosecution Service*

Frankreich: *Police Nationale und Tribunal Judiciaire de Paris*

Ukraine: *Nationale Polizei der Ukraine (Національна поліція України) und
Generalstaatsanwaltschaft der Ukraine (Офіс Генерального
прокурора)*

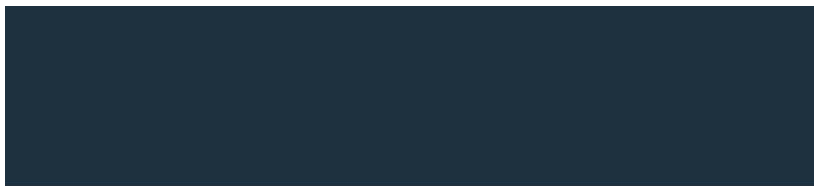
Litauen: *Büro der Litauischen Kriminalpolizei (Lietuvos kriminalinės policijos
biuras) und Generalstaatsanwaltschaft Litauen*

Koordinierung der internationalen Zusammenarbeit



Durch Eurojust koordinierte, regelmäßige Konferenzen zur
Entwicklungen gemeinsamer Strategien und zum
Informationsaustausch zwischen den Vertretern von Polizei
und Justiz aus den beteiligten Ländern unter Einbindung von
Vertretern von Europol





Herausforderungen und Lösungen

- Planung des internationalen Aktionstages mit gemeinsamen Maßnahmen in den einzelnen Ländern sowie im Wege der Rechtshilfe unter COVID-19-Beschränkungen
 - Einsatzzentren bei Europol und Eurojust mit Kollegen vor Ort sowie unterstützenden Videokonferenzen (beim BKA BAO)

Herausforderungen und Lösungen

- Rechtliche Ausgestaltung der Umleitung des Datenverkehrs der rein IP-basierten, sich ständig verändernden Emotet-Infrastruktur
 - „Hybrid-Beschluss“ mit Elementen der Beschlagnahme in Verbindung mit dem Einsatz technischer Mittel nebst Erstreckung auf neu entdeckte Systeme sowie
 - weitere Beschlagnahmebeschlüsse und Nutzung der Annexkompetenz

Herausforderungen und Lösungen

- Grenzen der rechtlichen und faktischen Umsetzungsmöglichkeiten der Maßnahmen in den beteiligten Ländern, insbesondere die rechtliche Übertragung der im Wege der Rechtshilfe erbetenen Maßnahmen (NL: „Legal Hacking“ aufgrund eines neuen Gesetzes)
 - Rechtshilfeersuchen der ZIT in enger Abstimmung mit den Kollegen aus den ersuchten Ländern (Niederlande, Ukraine und Litauen) erarbeitet

Herausforderungen und Lösungen

- Privatwirtschaft zur technischen Unterstützung
 - durch gutachterlich bestellte Sachverständige im hiesigen Verfahren

Stand der Ermittlungen

- Übernahme des Bot-Netzes durch konzertierte Aktion im Rahmen des internationalen Aktionstages am 26.01.2021
- Mehr als 50.000 IT-Systeme wurden auf die zur Beweissicherung eingerichtete Infrastruktur umgeleitet.
- Durchsuchungen beim Beschuldigten sowie zwei Zeugen in der Ukraine mit anschließenden Vernehmungen

Stand der Ermittlungen

- Beschlagnahme von Servern in Deutschland (Opfer-Kontroll-Seite und Distributionsseite) sowie in NL, USA, Kanada, UK, Frankreich, Litauen und der Ukraine
- Die Auswertung der Daten dauert an (Weitergabe bzw. Austausch nach zuvor vereinbartem H3-Handlingcode).

Folgemaßnahmen außerhalb des Ermittlungsverfahrens

- Weitergabe der ermittelten technischen Adressen der infizierten IT-Systeme an die Computer Emergency Response Teams (CERTs) (in Deutschland an das BSI), damit über diese die zuständigen Provider ermittelt und entsprechend informiert werden können, um ihrerseits ihre Kunden in Kenntnis zu setzen.
- Hilfestellung durch die CERTs zur Bereinigung der IT-Systeme (Einbeziehen der Anbieter von AV-Lösungen).

25. April 2021 – Tag der Wahrheit

- Die seitens der Strafverfolgungsbehörden in die vormals tätereigene IT-Infrastruktur eingebrachte Binärdatei hat das Ausführen aller Prozesse und ihre Persistenz beendet.
- Die tätereigene Emotet-Binärdatei verbleibt auf dem jeweiligen IT-System in Quarantäne.
- Zusätzliche Unterstützung zur Bereinigung ist durch Veröffentlichung einer YARA-Signatur auf der Homepage des BKA am 16.04.2021 erfolgt.

**Vielen Dank für Ihre Aufmerksamkeit!
Fragen und Anmerkungen?**