Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) -

HESSEN

Gefangen im Netz?
Internetkriminalität im Wandel als stete Herausforderung für die Strafverfolgungsbehörden

Online-Vortrag für die Gesellschaft für Informatik e. V. am 20. Juli 2022

Foto: James Thew / Fotolia

Staatsanwältin Linda Bertram

HESSEN

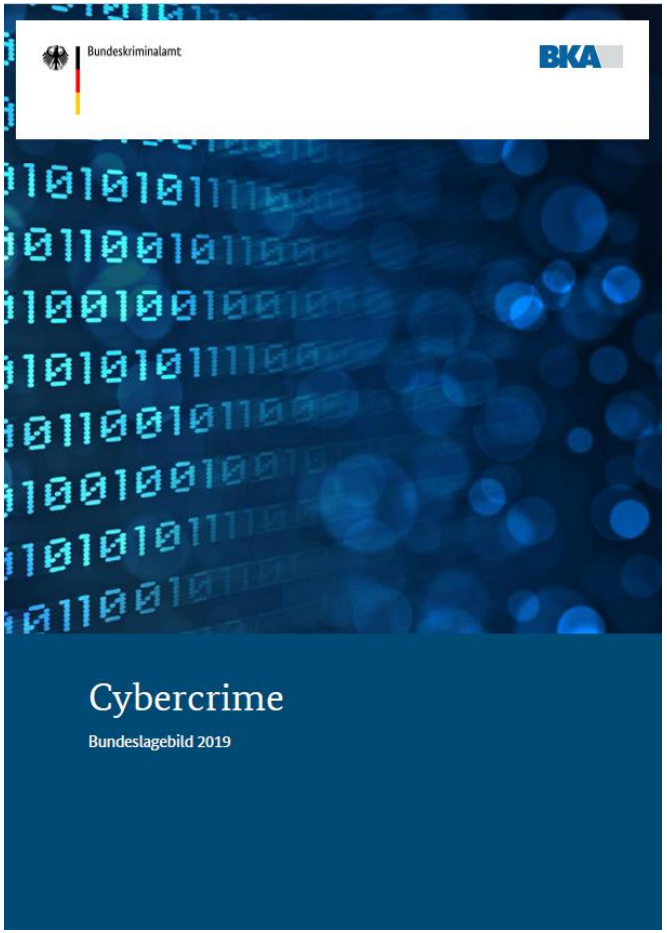
Cybercrime wird immer professioneller

ca. 1 Mrd.
identifizierte Malware-familien

ca. 114 Mio.
neue Malware-Varianten in 2019

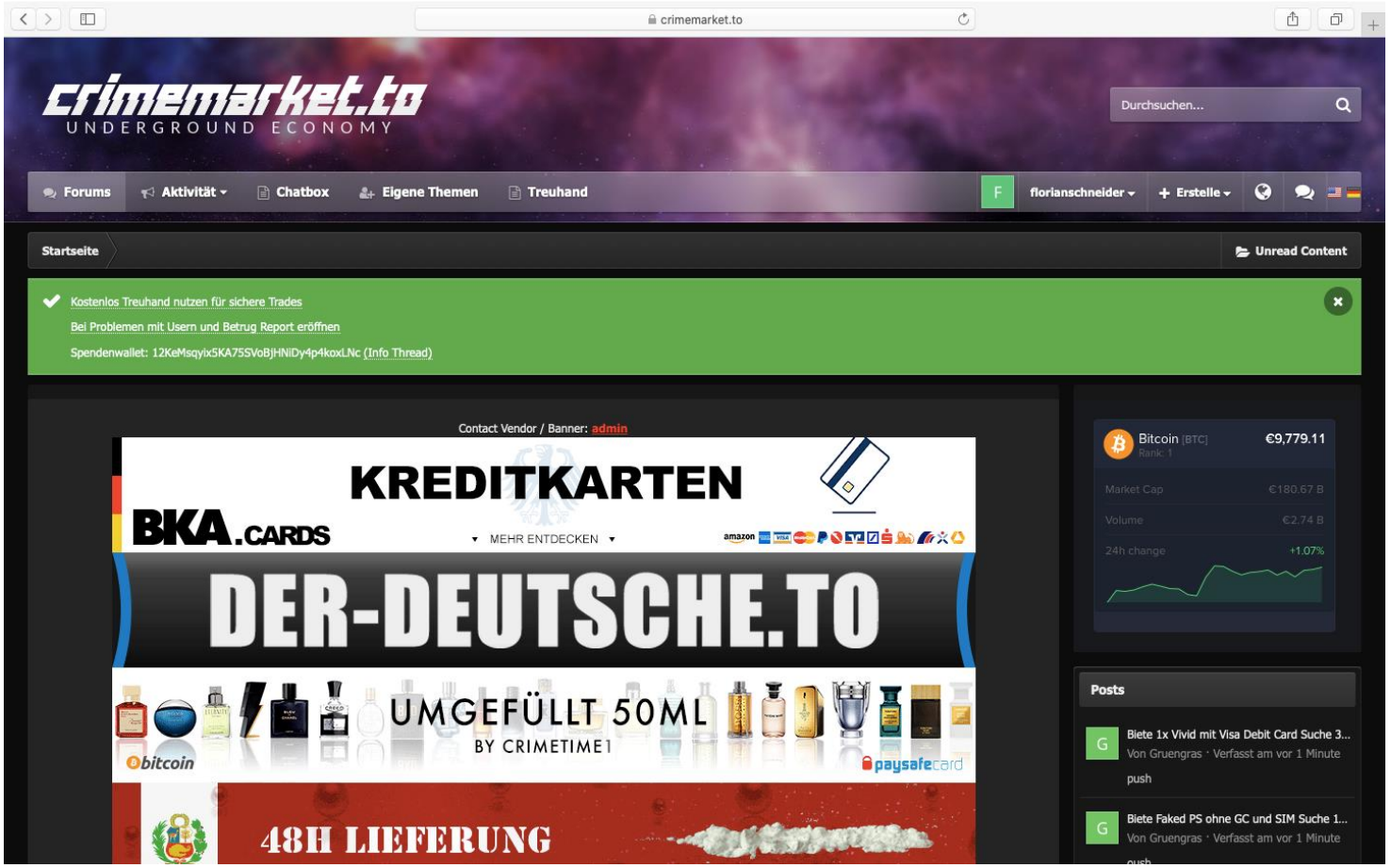
ca. 8 bis 17 Mio.
neue Malware-Varianten im Monat

ca. 312.000
neue Malware-Varianten pro Tag



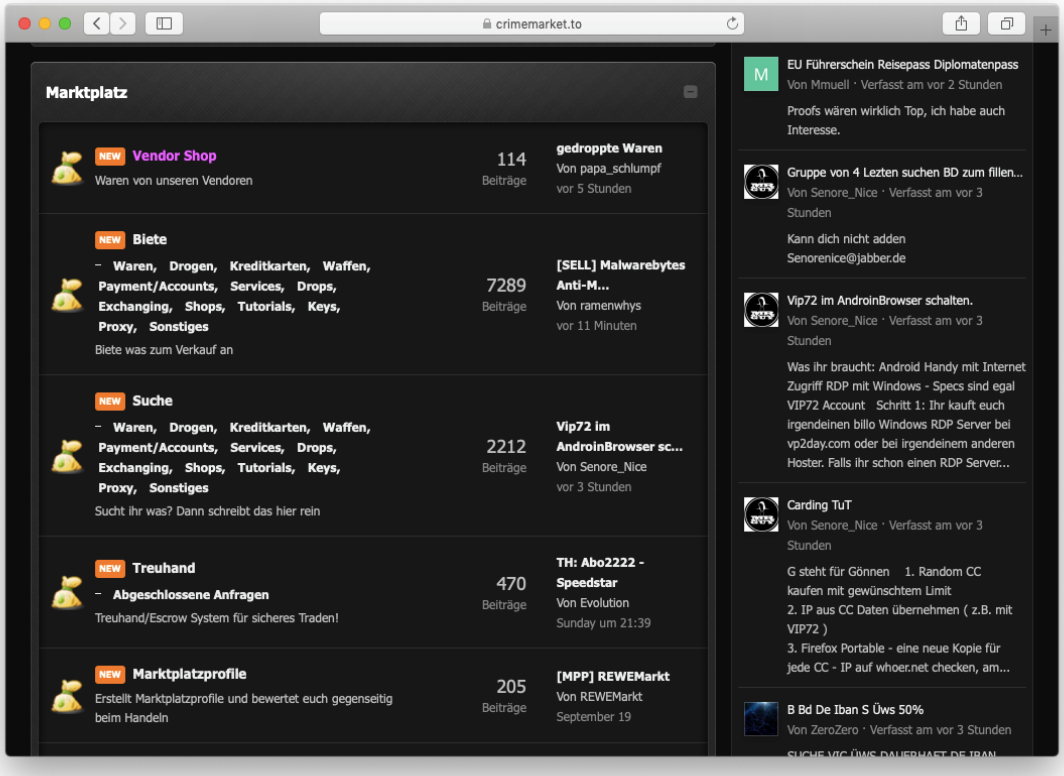
HESSEN

Cyberkriminelle müssen keine Informatiker sein – Crime as a service



HESSEN

Cyberkriminelle müssen keine Informatiker sein – Crime as a service

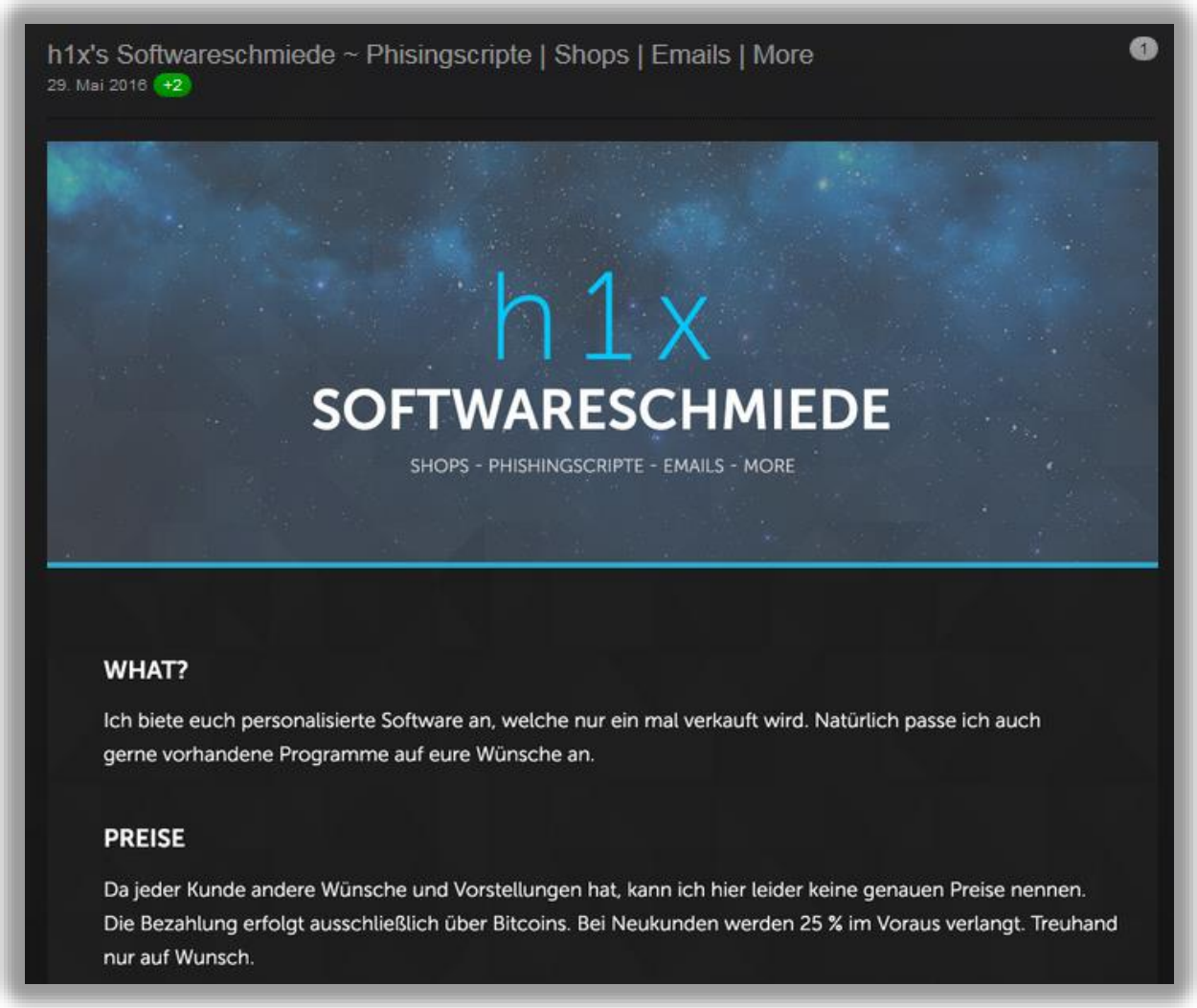


HESSEN

Cyberkriminelle müssen keine Informatiker sein – Dienstleistung für Erpressung/Computersabotage

HESSEN

Handel mit Schadsoftware

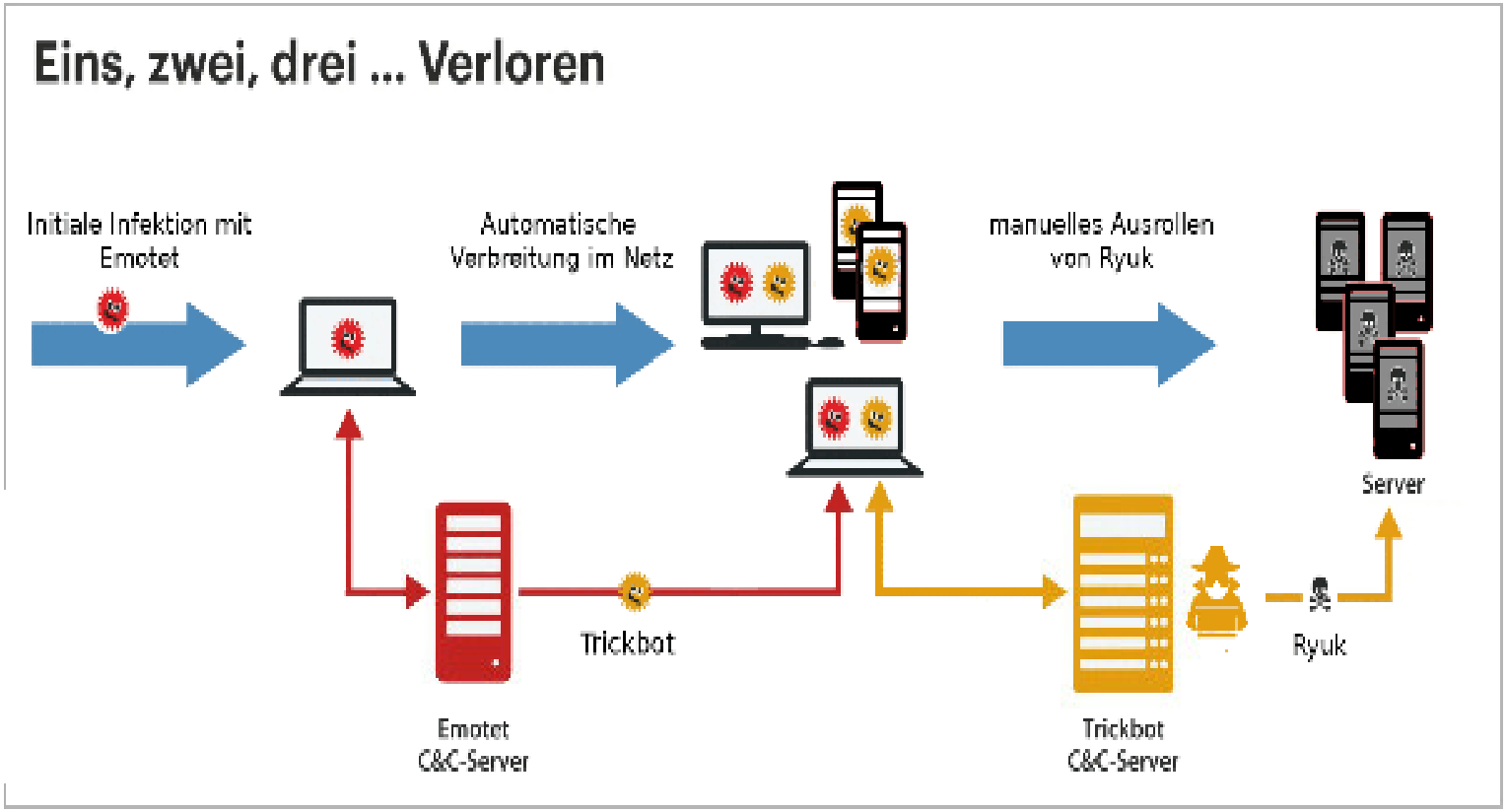


HESSEN

Quelle:Sophos

HESSEN

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)

HESSEN

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

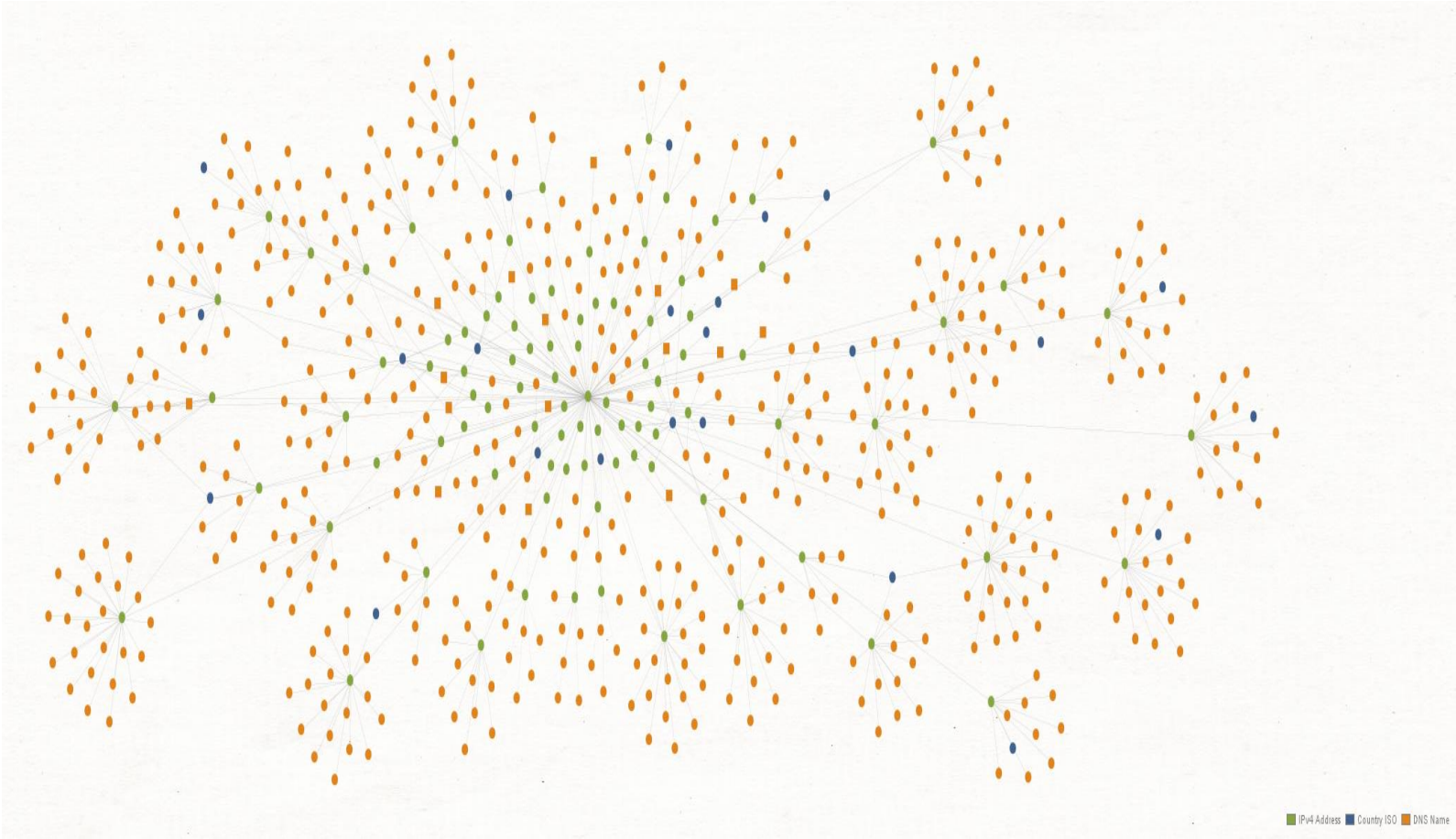
HESSEN

Der Beginn unseres Verfahrens

- Server-Standortin 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

HESSEN

Die Emotet-Infrastruktur



HESSEN

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*

HESSEN

Koordinierung der internationalen Zusammenarbeit

EUROJUST

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

EUROPOL

HESSEN

HESSEN

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)

HESSEN

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

HESSEN

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

HESSEN

Herausforderungen und Lösungen

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

HESSEN

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

HESSEN

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).

HESSEN

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).

HESSEN

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.

HESSEN

Vielen Dank für Ihre Aufmerksamkeit!
Fragen und Anmerkungen?