Corporate Loader "Emotet": History of "X" Project Return for Ransomware

advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware

AdvIntel November 19, 2021

- Nov 19, 2021
-
- 7 min read

By Yelisey Boguslavskiy & Vitali Kremez

AdvIntel deep-dives into the contemporary threat landscape illustrating how Emotet's return might re-shift the ransomware ecosystem.

Executive Summary - Why Corporate Loader Returned?

The November 14, return of Emotet (project "X" internally) correlates with two long-term developments in the ransomware ecosystem: 1) unfulfilled loader commodity demand 2) decline of the decentralized RaaS (Ransomware-as-a-Service) model, and the return of the monopoly of organized crime syndicates such as Conti.

AdvIntel's visibility into the adversary space enables us to confirm that it was the former Ryuk members who were able to convince former Emotet operators to set up a backend and a malware builder from the existing repository project to return to business in order to restore the TrickBot-Emotet-Ryuk triad. This partnership enables the Conti syndicate to answer the unfulfilled demand for initial accesses on an industrial scale, while competitor groups such as LockBit or HIVE will need to rely on individual low-quality access brokers. As a result, Conti can further advance their goal of becoming a ransomware monopolist.

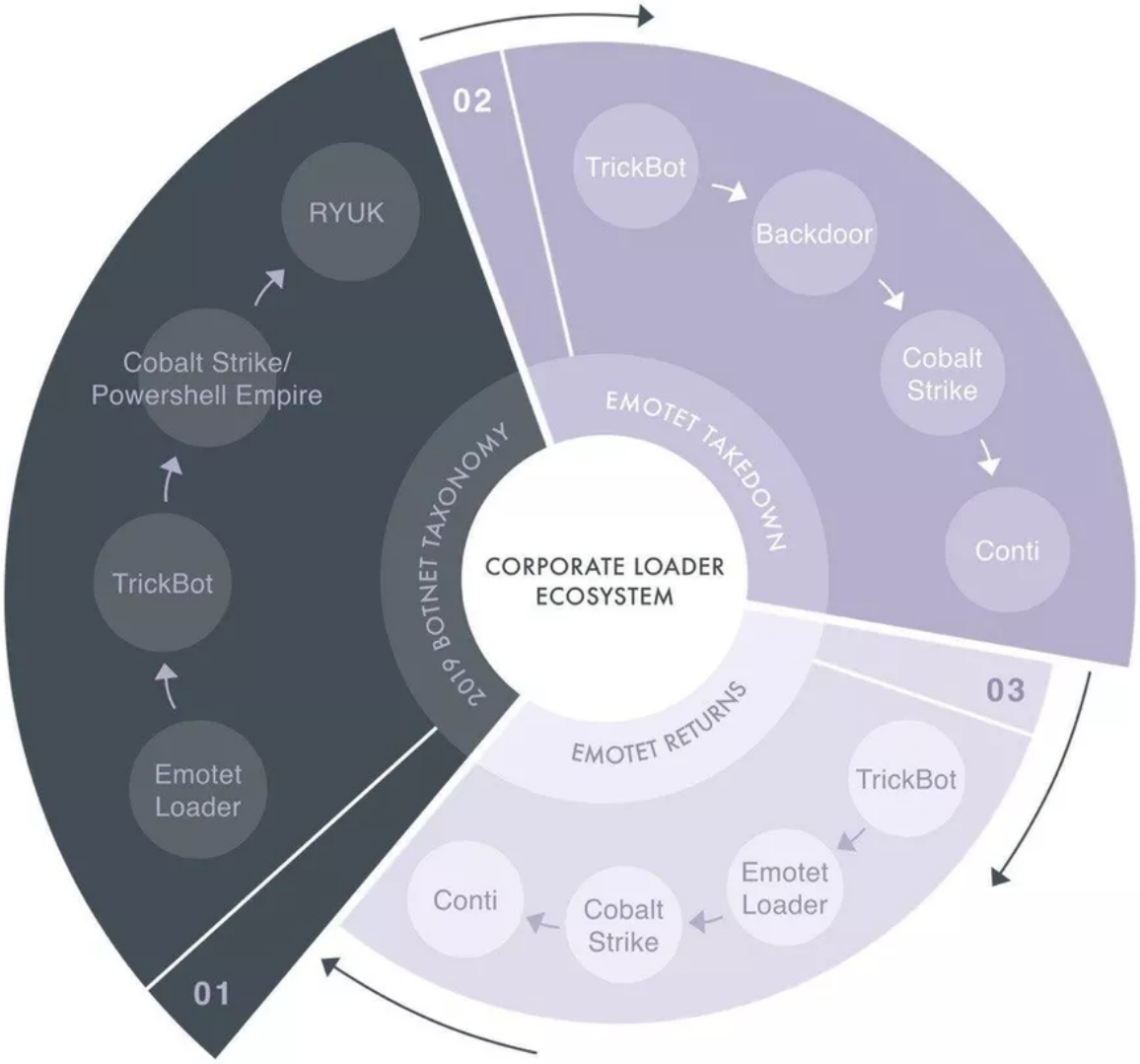


Image 1: Emotet progression from ransomware partnership taxonomy.

Threat Landscape

On November 14, AdvIntel identified the return of the Emotet loader which has been inactive since January 2021 after a law enforcement takedown. AdvIntel's investigative hypothesis is that this return has been shaped by the contemporary ransomware landscape and will have a major impact on the development of ransomware.

This resurgence of Emotet will likely cause the largest threat ecosystem shift in 2021 and beyond due to three reasons:

1. Emotet’s unmatched continuous loader capabilities
2. The correlation between these capabilities and the demanded of the contemporary cybercrime market
3. The return of the TrickBot-Emotet-Ransomware triad resulted from the first two points.

Emotet - “The Most Dangerous Loader”

Emotet is a loader botnet and a criminal syndicate managing this botnet using a loader-as-a-service model. This means that Emotet offers the capabilities of a loader to deliver the payload of its customer.

Emotet became successful in developing this model (and in choosing the “right” ransomware customers); the Department of Homeland Security defined it as one of the most costly and destructive forms of malware, leaving no sector from government to private industry safe.

Emotet’s strategic, operational, and tactical agility was executed through a modular system enabling them to tailor payload functionality and specialization for the needs of specific customers. At the same time, Emotet operators leveraged understanding of social issues and conflicts that enabled them to weaponize the socio-political domain for email spam campaigns.

Overall, Emotet's success was constituted by three things.

1. Technical delivery of the payload
2. Creative and persistent approach to spam dissemination
3. Alliances with top-tier groups such as TrickBot and Ryuk

Unfulfilled “Corporate” Loader Demand

Most likely because no other groups were able to replicate such capabilities, after leaving cyberspace in January 2021, Emotet left a vacuum that was not filled even with MASSLOADER, also known as Hancitor. Other botnets like QBot attempted to step in but largely failed as a persistent and continuous loader system.

This created a major interruption within the ransomware supply chains.

After the takedown of Emotet, the demand for an efficient source of high-quality access and advanced dissemination was not matched with a proper supply. According to AdvIntel's sensitive source intelligence, even top-tier groups who have their venues for organized access supply-chains such as **Conti** (relies on **TrickBot**, **BazarLoader**, and **Cobalt Strike** spam delivery) or **DoppelPaymer** (relies on **Dridex**) express concerns regarding the lack of initial accesses.

This discrepancy between supply and demand makes Emotet's resurgence important. As this botnet returns, it can majorly impact the entire security environment by matching the ransomware groups' fundamental gap.

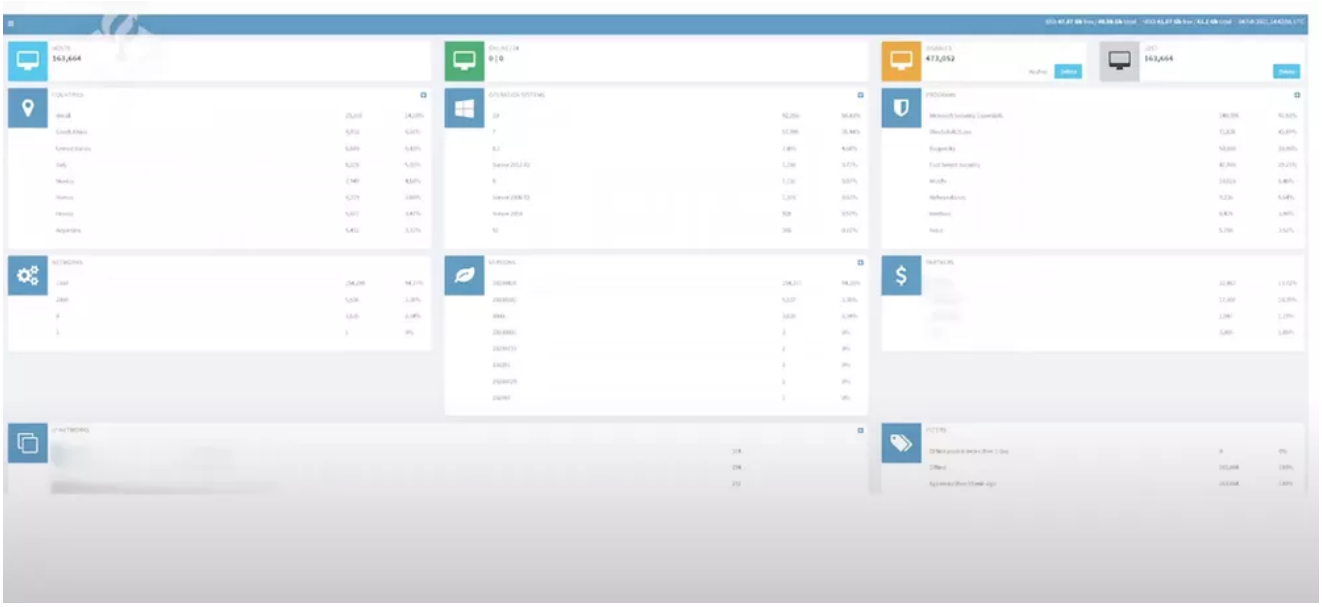


Image 2: Emotet backend displays the partnership profit cut.

Ransomware Market Monopolization

In the Spring and Summer of 2021, most of the major **ransomware-as-a-service (RaaS)** groups including **REvil**, **Darkside**, **Avaddon**, **Blackmatter**, **Babuk**, and others quit the criminal market. Remaining groups such as **LockBit** and **HIVE** faced a major decline in payments from victims due to extensive use of backups and more advanced defenses.

This decline of RaaS made the ransomware landscape look closer to its pre-2019 shape in which long-term strategic criminal partnerships between top-tier organized crime groups enabled unprecedented revenues. This possibly motivated larger groups including Conti which has been fulfilling the vacuum left by REvil and other RaaSes to consider reestablishing the Emotet liaison.

This prospective partnership could be motivated by a major success of a previous alliance achieved in 2018 between **Emotet**, **TrickBot**, and **Ryuk**. These centralized, highly organized groups with advanced technical and social skills primarily relied on encryption skills, high discipline, teamwork, division of labor, and the highest levels of centralization and organization. After joining efforts, they dominated the cybercrime environment up until 2019.

In 2019-2021, this monopoly was challenged by RaaSes, their decentralized affiliates, and their emphasis on data exfiltration and not data encryption. However, after two years this model started to prove unsustainable.

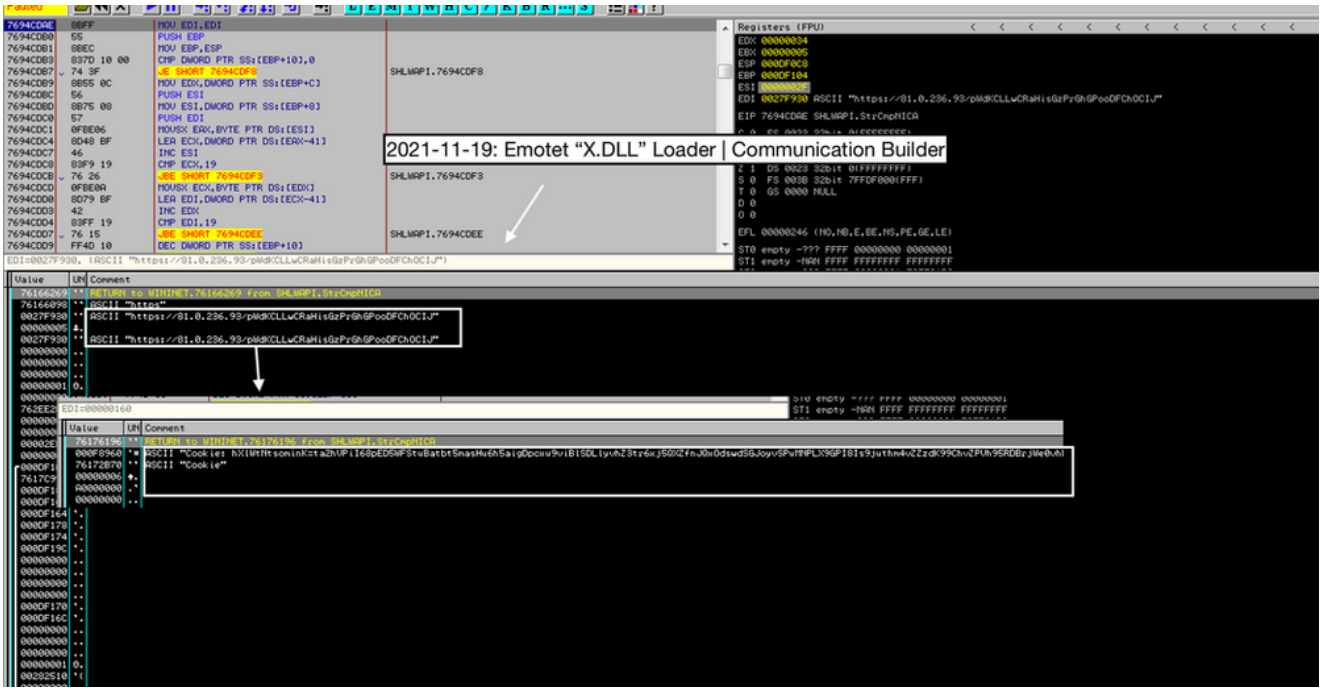
Exit-scams, lack of proper coordination and organization (greedy affiliates attacking critical industry such as Colonial Pipeline), affiliates using low-level access sellers and brokers, and other organizational challenges lead to RaaS closings by late 2021. Moreover, simple data theft, which was at the center of RaaS models, briefly led to the situation in which the victims simply allow criminals to dump the data and decline to pay the ransom.

With RaaSes disappearing, traditional groups: Ryuk (in the form of Conti), TA505, and EvilCorp regained their dominance in the threat hierarchy. They have become the center of gravity for the talented malware specialists who are massively leaving disbanded RaaSes in order to find a stable and ordered operational environment.

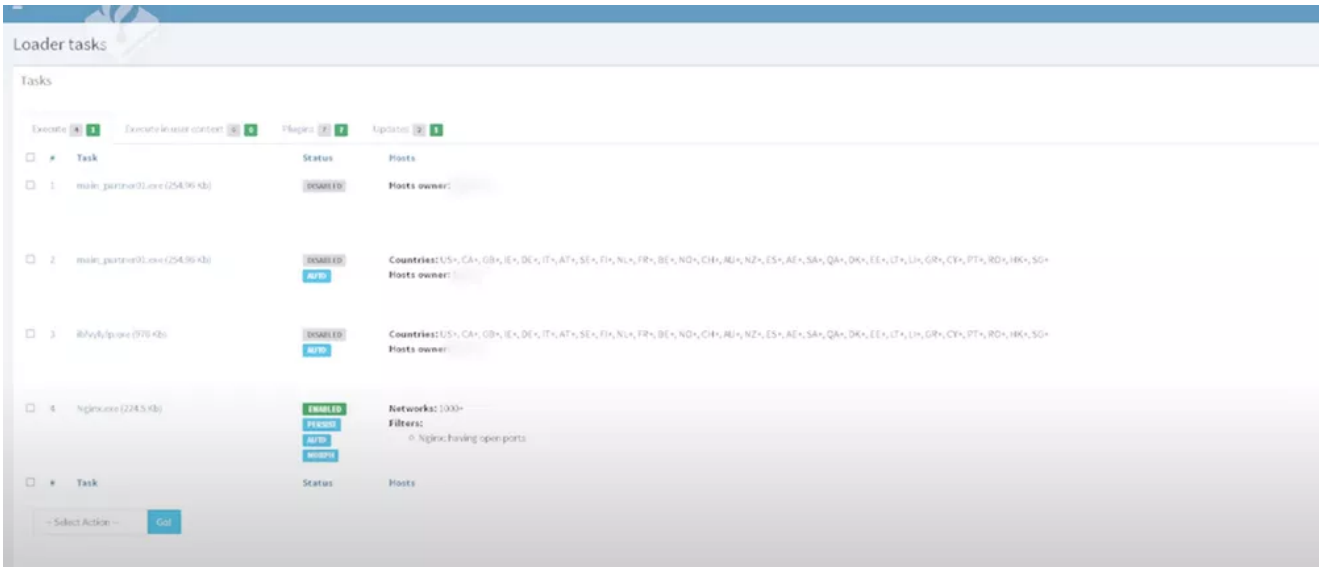
This new environment made Emotet's return a highly anticipated event. For Conti, the syndicate had full capacity to approach Emotet once again, being the ransomware "top-dog", they already had Ryuk's former member on board and had maintained the alliance with TrickBot. Emotet was the last missing part.

The Newer Crime Triad

As the threat environment is returning to its pre-2019 shape, we see a resurgence of the crime triad that was the pinnacle of the traditional ransomware model - **Emotet-TrickBot-Ryuk**. In the 2021 landscape, the triad is renewed as **TrickBot-Emotet-Conti.**



In November 2021, AdvIntel utilized our unique visibility into the TrickBot adversarial domain in order to spot a major threat shift: Emotet's partner loader program began resourcing existing TrickBot infections. In other words, TrickBot began dropping Emotet loaders. The Emotet compilation timestamp is Sun Nov 14 14:50:34 2021 UTC. The unpacked core is known as "X.dll" with the export function "Control_RunDLL"



Source: https://twitter[.]com/VK_Intel/status/1460308855129313281

At this point, AdvIntel assesses with a high level of confidence that the Conti syndicate will or is establishing a new partnership with Emotet and is planning to actively expand the loader operations. This is especially important as Conti is known to rely on sustainable methods of operations, one of which is a holistic locker lifecycle starting with initial access and ending with victim negotiations. It is likely that this holistic approach and guarantees of operational security may become a convening point for Emotet. More importantly, this means that Emotet will likely work with Conti in an exclusive manner.

At the same time, Emotet's liaison can solve Conti's major demand in loader commodities and initial accesses. Moreover, it even further positions Conti as a dominating player in the threat landscape. RaaS groups - Conti's competitors - rely primarily on massive dissemination of low-quality spam, abuse of vulnerable and exposed RDPs, and abuse of vulnerable VPNs. The majority of the RaaS offensive capabilities come from affiliates who were tasked to harvest initial access themselves and most often relied on underground low-quality credential and log sellers.

Even though, initially, this model enabled a spray-and-pray targeting vulnerable endpoints without major effort, by 2021, patching, increasing cyber hygiene, more proper audits, and other defensive actions made it infeasible to rely on the affiliate-driven attacks.

This makes Emotet's persistent spam campaigns a competitive advantage for the Conti group.

Conclusion

Emotet's return is not coincidental, it is caused by major shifts in the overall cybercrime domain. The growing monopolization of the ransomware world, which is rapidly conquered by only a few highly-organized criminal corporations, leads to better opportunities for criminal ventures like the Emotet botnet developers.

Larger organized crime groups have higher profits working together in a liaison. This has been proven by the alliance of **TrickBot**, **Emotet**, and **Ryuk**: the three major players of the pre-2019 cybercrime hierarchy. In late 2021, as the smaller actors are losing their impact and power, while larger ones are becoming even bigger, the new criminal alliance between **TrickBot**, **Emotet**, and **Conti**, is a logical avenue for criminals.

This can become the largest adversarial shift in the last five years since the Emotet attempted takedown in January 2020.

Indicators of Compromise (IOCS):

The attached MISP JSON and CSV IOC exportable documents are available.

2021-11-18-ADVINTEL-EMOTET-misp.event.vk.7734.json

.txt

Download TXT • 119KB

2021-11-18-ADVINTEL-EMOTET-misp.event.vk.7734

.csv

Download CSV • 2KB

Attack Pattern

- Spearphishing Attachment - T1193
- Spearphishing Link - T1192
- Command-Line Interface - T1059
- Execution through Module Load - T1129
- Create Account - T1136
- Access Token Manipulation - T1134
- Code Signing - T1116
- New Service - T1050
- Scripting - T1064
- Rundll32 - T1085
- Regsvr32 - T1117
- Regsvcs/Regasm - T1121
- PowerShell - T1086
- Mshta - T1170
- XSL Script Processing - T1220
- Kerberoasting - T1208
- Credential Dumping - T1003
- Network Share Discovery - T1135
- Password Policy Discovery - T1201
- File and Directory Discovery - T1083
- Domain Trust Discovery - T1482
- Account Discovery - T1087
- System Information Discovery - T1082
- Pass the Ticket - T1097

- Pass the Hash - T1075
- Exploitation of Remote Services - T1210
- Data Staged - T1074
- Email Collection - T1114
- Man in the Browser - T1185
- Data Obfuscation - T1001
- Data Encoding - T1132
- Multi-hop Proxy - T1188
- Data Encrypted - T1022
- Automated Exfiltration - T1020
- Exfiltration Over Command and Control Channel - T1041
- Data Encrypted for Impact - T1486

Course of Action

- Automated Exfiltration Mitigation - T1020
- Bypass User Account Control Mitigation - T1088
- Credential Dumping Mitigation - T1003
- Custom Command and Control Protocol Mitigation - T1094
- Email Collection Mitigation - T1114
- Exfiltration Over Alternative Protocol Mitigation - T1048
- Exfiltration Over Command and Control Channel Mitigation - T1041
- Multilayer Encryption Mitigation - T1079
- Pass the Hash Mitigation - T1075
- Pass the Ticket Mitigation - T1097

*Our proprietary platform, **Andariel**, provides a mirrored view of criminal and botnet activity, which supplies our users with predictive insight that* is *used to prevent intrusions from maturing into large-scale threat events such as ransomware attacks.*