Suspected Conti Ransomware Activity in the Auto Manufacturing Sector

dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/

March 16, 2022

Blog Post

By Josh Hanrahan

03.16.22

Dragos has observed consistent network communication between Emotet Command and Control (C2) servers and numerous auto manufacturing companies. These Emotet servers are suspected to be controlled by the Conti ransomware group.

At this stage, Dragos has not yet observed any confirmed initial access methods being utilized and does not have any evidence of ransomware encryption being initiated. The observed communications from the networks are consistent with those commonly associated with established footholds. Dragos observed this activity starting in December 2021, but it may have begun prior to that. It has been ongoing until March 2022.

If systems located in levels 2 to 3 of the Purdue Model such as engineer workstations, historians, or Supervisory Control and Data Acquisition (SCADA) systems suffer a ransomware infection, the impact on industrial operations can be severe. Additionally, any ransomware infection occurring on systems in Level 4 of the Purdue model such as Domain Controllers, File Servers or Web Servers can sever key business processes that industrial operations may be reliant upon.

Key Findings

- Dragos is observing evidence of multiple automotive manufacturers compromised by Emotet, a malware strain and a cybercrime operation, which has precipitated ransomware events in the past.

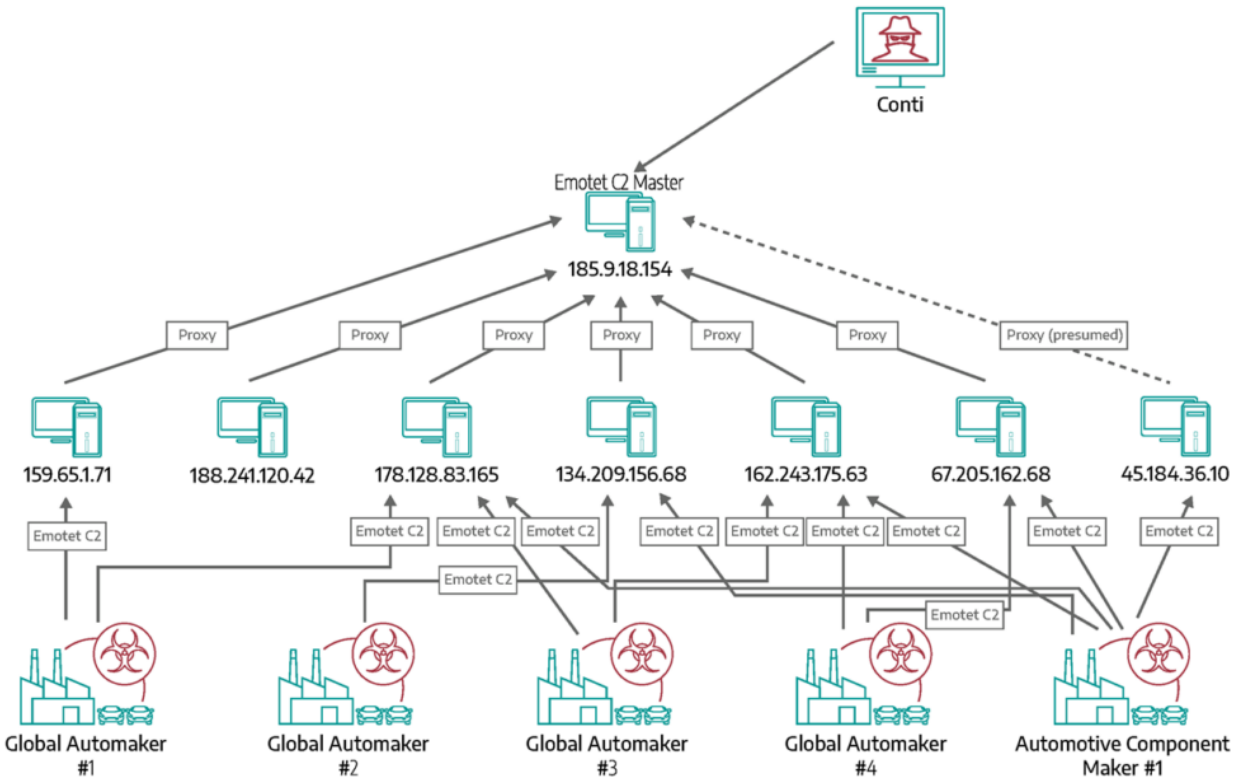
- Dragos investigated the Internet Protocol (IP) addresses detailed on twitter by the user @ContiLeaks. This user appears to be someone with potential insider knowledge of the Conti ransomware group who is leaking information due to disagreeing with Conti's public support of the Russian invasion of Ukraine.
- Dragos examined the IP addresses in the tweets and noted copious amounts of communication to confirmed Emotet C2 nodes.
- Dragos observed numerous automotive organizations across North America and Japan frequently communicating with the Emotet C2 servers.

CONTI & EMOTET Adversary Infrastructure

Dragos analyzed network telemetry associated with the suspected Conti master C2 server and observed frequent communication between it and a subset of IP addresses that are Emotet C2 nodes, as shown below.

Network Indicator	Description
82.202.192[.]66	SELECTEL-MSK – Emotet C2
67.205.162[.]68	Digital Ocean – Emotet C2
188.241.120[.]42	BANDWIDTH-AS – Emotet C2
185.9.18[.]154	M247 – Suspected Conti master C2 server
178.128.83[.]165	Digital Ocean – Emotet & legacy Dridex C2
162.243.175[.]63	Digital Ocean – Emotet C2
159.65.1[.]71	Digital Ocean – Emotet C2
134.209.156[.]68	Digital Ocean – Emotet C2
159.89.230[.]105	Digital Ocean – Emotet C2
45.184.36[.]10	AS269305 – Emotet C2

CONTI & EMOTET Infrastructure
Dragos further examined network communications between the Emotet C2 nodes and any other IP addresses, which subsequently highlighted traffic consistent with C2 communications between potential victims and the Emotet C2 servers. Figure 1 below shows our observations.



Adversary Infrastructure

Victimology

Analysis of the network telemetry from the C2 nodes highlighted continued communication to and from automotive related organizations in North America and Japan, including but not limited to:

- Three of the world's top automakers
- A key domestic supplier to one of the world's top automakers
- An automotive component manufacturer

Not only did victims exhibit network communication consistent with C2 activity to one IP address, but some victims were communicating with many of the C2 IP addresses. This indicates that initial access footholds into these victim's networks were well established and have multiple backup controllers if some were to go offline.

Dragos has contacted the organizations affected and advised them to enact their incident response playbooks for ransomware events.

Recommendations from Dragos Experts

Ransomware can impact critical business functions across both Information Technology (IT) environments and Operational Technology (OT) environments. If an adversary gains a foothold and systems across the network are encrypted, business and operational processes can be severely halted, in turn causing a reduction in or cessation of critical operations.

Dragos advises that IT and OT security staff review the details of this activity in conjunction with their organizations threat modelling and determine any follow-up actions if appropriate.

Dragos also advises that the following action items may be helpful in mitigating or detecting ransomware events against your network:

- Hunt for ransomware related indicators of compromise on externally facing third-party managed devices as well as organization managed devices that have logging available.
- Monitor for key Tactics, Techniques and Procedures (TTPs) utilized by ransomware adversaries. The following techniques, mapped to MITRE's ATT&CK for Industrial Control Systems (ICS), were observed in this activity: T0885: Command and Control – Commonly Used Port.
- Monitor network traffic for TTPs where prevention methods may be missing malicious activity. For example, software misconfiguration of firewalls or web proxies. Additionally, with C2 communication over common ports such as 80 (HTTP) or 443 (HTTPS), analysis of bytes transferred outwards, abnormal user-agents, or connection initiation at a repeated interval can highlight potential C2 beaconing activity.
- Monitor East-West network traffic for relevant TTPs and assess if the details of the traffic are in line with normal baseline behaviors.
- Assess IT and OT connectivity and exposure: Use best practices to secure sections of your network.
- Assess your network architecture and security controls separately.
- Keep Systems Fully Patched: Patch your IT and OT systems where and when it makes sense to mitigate vulnerabilities.
- Regularly Back up Files to Remote Servers: Restoring your files from a backup is the fastest way to regain access to your data.
- Use Security Solutions: Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering.
- Ensure networks are properly segmented with separate authentication infrastructure for IT and OT.
- Ensure least privileges and leverage user access control: Implement practices to prevent adversary lateral movement and deployment of ransomware in the industrial environment. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only the resources required to perform routine, legitimate activities.

- Revise or create your incident response plan on how to respond to ransomware events.

References

The Dragos 2021 Year in Review

Find proactive, actionable information, and defensive recommendations from the frontline team safeguarding civilization from cyber attacks.

Prepare Your Cyber Defenses