Dragos ICS/OT Ransomware Analysis: Q4 2021

dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

February 9, 2022

A common misconception suggests ransomware is solely a threat to information technology (IT); however, data from 2021 indicates ransomware is having an increasing impact on operational technology (OT) as well.

Ransomware can cause OT impacts in four ways:

1. In the case of Colonial Pipeline, operators preemptively shut down their operations to prevent enterprise IT ransomware from spreading into OT. This strategy, while causing disruption, preserves OT from potential long-term downtime caused by a successful ransomware infection.
2. Flat networks and lack of asset visibility create an environment where ransomware can spread quickly through both IT and OT networks.
3. Dragos is aware of six ransomware strains that possess built-in OT kill processes: Cl0p, MegaCortex, Netfilim, LockerGoga, Maze, and EKANS. While Ransomware actors often use process kill lists to target security products in IT networks, in the context of OT networks the adversaries kill processes which are critical to OT functions and which might otherwise prevent the ransomware from encrypting critical files used by the OT programs.
4. Ransomware attacks that impact enterprise IT systems only, but lead to the release of proprietary documentation on OT technology on underground forums if the ransom is not paid, could lead to follow-on attacks targeting OT technology directly by cybercriminals or state-sponsored actors.

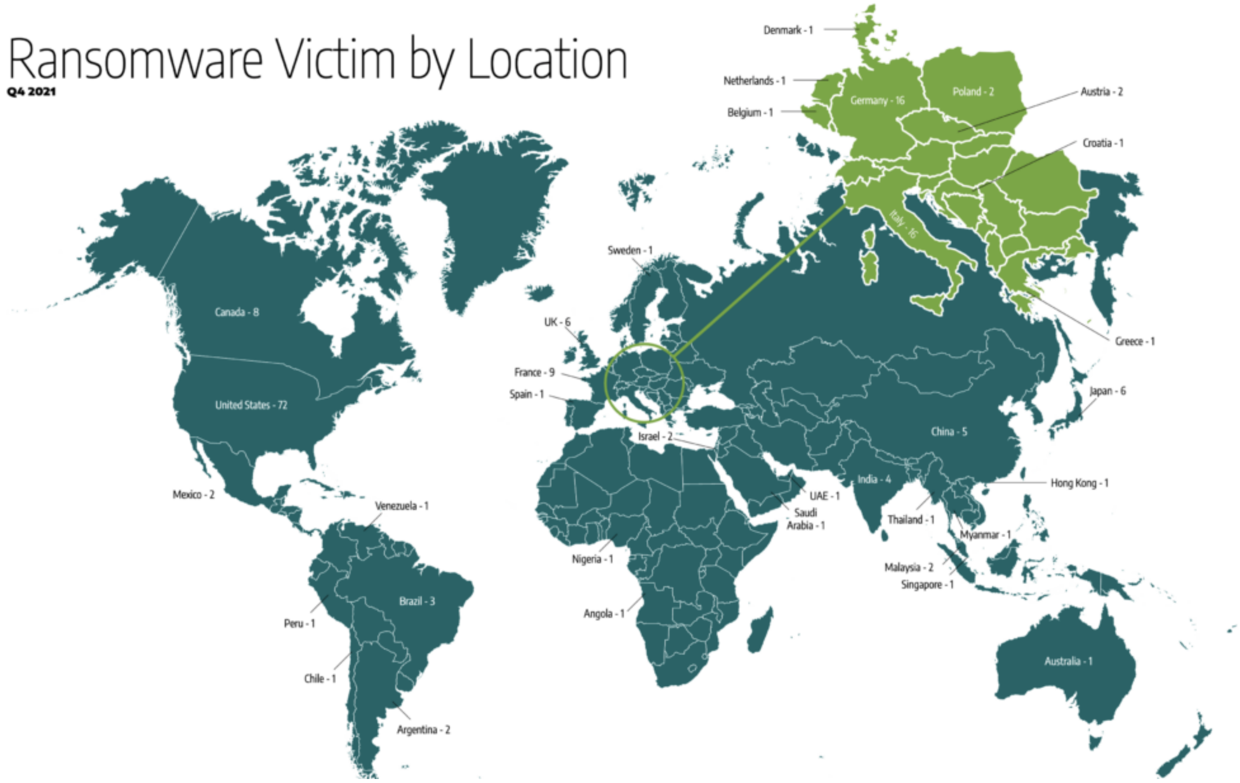
Dragos analyzed data from 37 ransomware strains on Dark Web resources leveraged to post victims, leak files, and conduct negotiations. Appearance on a Dark Web resource does not confirm that ransomware actors successfully compromised a firm, the extent of access achieved by the ransomware actors, or whether a firm made the ransomware payment. Occasionally, ransomware actors will post inaccurate information on Dark Web resources; for example, listing the name of one firm and the description of a completely different firm. This may be accidental, or an attempt to cause confusion amongst victims.

In some cases, ransomware actors will attempt to appear to have compromised a victim by cross-posting documents identified as part of a different ransomware breach, as was the case with Schneider Electric and Vestas. While Dark Web resources are not fully accurate, they provide unique insight into the priorities of ransomware groups, including which sectors and sub-sectors they most frequently target, which sectors they prioritize, and which areas of the globe are more likely to experience attacks.

Dragos observed the following trends in Q4 2021 (October, November, and December).

Ransomware Victim by Location

Globally, 41% of postings featuring victims located in the U.S.; Germany and Italy tied for second with 9% of activity respectively.

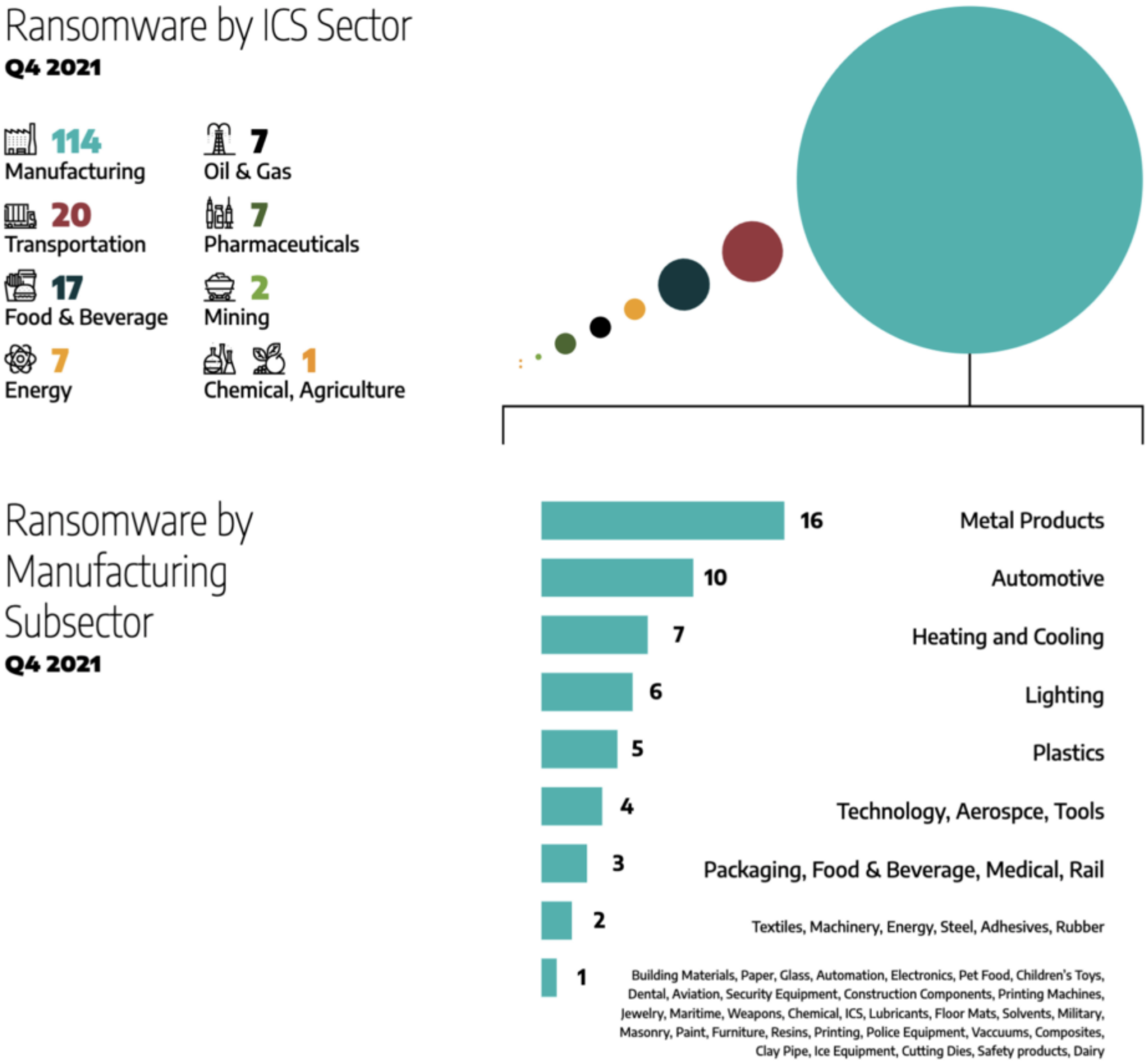


Activity stayed consistent each month, with 58 Industrial Control Systems (ICS) Dark Web postings in October, 57 in November, and 61 in December for a total of 176. However, individual group activity spiked month to month, with Grief posting seven of their 13 ICS victims in October, one in November, and five in December; notably, all but one Grief postings were victims in the Manufacturing sector. Additionally, PYSA activity spiked in November with 11 ICS victim postings across sectors including Oil and Gas, Food and Beverage, and Transportation; Dragos observed 13 total PYSA victim postings during this timeframe.

Ransomware by ICS Sector

By sector, 65% of postings featured victims in the Manufacturing sector, which is consistent with data collected starting 1 June 2021. Dragos identified 52 unique manufacturing sub-sectors during this timeframe. By sub-sector, 14% of victims were in metal product

Manufacturing, 9% were in automotive Manufacturing, and 7% were in technology Manufacturing.

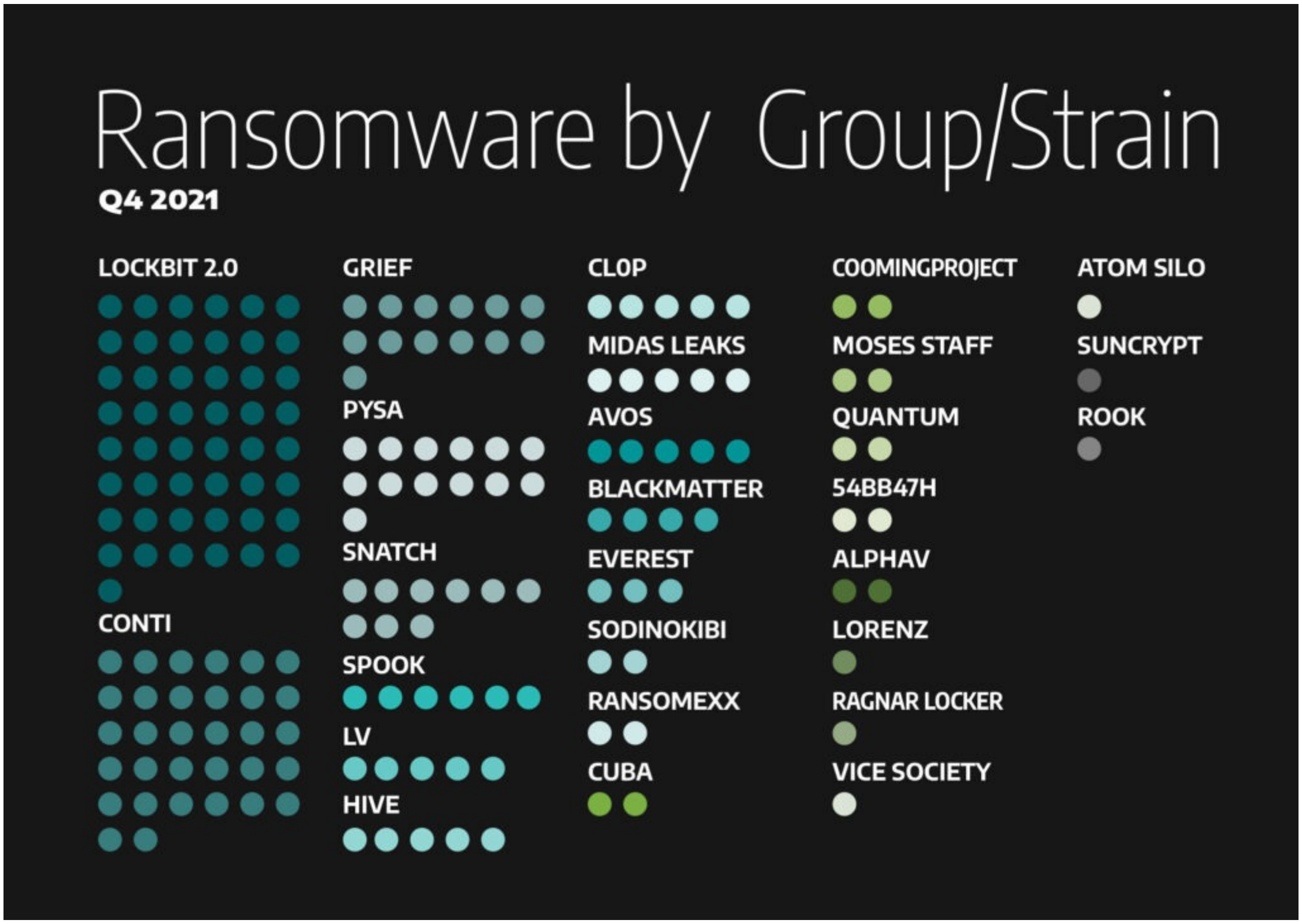


Ransomware attacks against the Manufacturing Sector may cause upstream and downstream disruption to transportation companies and other sectors dependent on manufacturing output, including food and beverage, automotive firms, energy firms that leverage metal products, and technology firms. For example, a successful attack against a manufacturer of automotive parts may halt further production of vehicles leveraging that component.

Following Manufacturing, 10% of attacks featured victims in the Transportation Sector, 10% featured the Food and Beverage sector, and 4% each featured Energy, Pharmaceuticals, and Oil and Natural Gas.

Ransomware by Group or Strain

Analyzing the data by ransomware strain, Lockbit 2.0 made 28% of postings and Conti made 18% for a total of 46% between the two groups. Interestingly, PYSA's November activity spike nearly tied Conti's number of attack victims in the same period, with 11 ICS victims to Conti's 12. This is not true for any other month. 81% of Conti's ICS Dark Web postings featured the manufacturing sector.



Lockbit 2.0 Ransomware Threat Behavior

In June, Lockbit 2.0 developers launched a Ransomware-as-a-Service (RaaS) program to enable affiliates to leverage the platform to conduct ransomware attacks.[1] The platform uses a double extortion model, where data is exfiltrated prior to systems being locked; if the victim refuses to make a payment, attackers will threaten to leak the exfiltrated data. The affiliates who conducted the attack and the developers of the ransomware split any ransom payments between themselves. Lockbit is believed to be related to the LockerGoga and MegaCortex ransomware families due to shared tactics, techniques, and procedures, particularly the ability to propagate automatically to new targets.

According to an article published on 4 August, Lockbit is actively recruiting corporate insiders to provide Remote Desktop Protocol (RDP), Virtual Private Network (VPN), and email credentials to assist attackers in gaining access to networks in exchange for million dollar payouts.[2] Lockbit does not operate in countries that are formerly a part of the Soviet Union and leverages tools such as StealBIT, Metasploit Framework, and Cobalt Strike.[3] In late July, reports emerged indicating researchers had uncovered a new version of the of the

Lockbit 2.0 ransomware platform that automates the encryption of a Windows domain using Active Directory group policies.[4] Dragos assesses with low confidence Lockbit, and subsequent iterations of this ransomware group, will continue to develop innovative techniques to increase potency of ransomware operations.

Conti Ransomware Threat Behavior

Conti is also a Ransomware-as-a-Service (RaaS) platform; however, a September report by Cybersecurity and Infrastructure Security Agency (CISA) notes a variation in its structure as deployers are likely paid a wage rather than a percentage of the profits in the event the ransom is paid.[5] Techniques used by Conti are not especially unique; for example, they maintain persistence using Cobalt Strike or Powershell. However, unlike many ransomware groups who focus on building the reputation that victims will receive their files if the ransom is paid, Conti is significantly more volatile, occasionally not returning files after victims pay the ransom or only returning a fraction of compromised files.

In August 2021, an alleged Conti affiliate leaked the group's "playbook" after apparently not receiving full payment following an attack; researchers who viewed the playbook advised network administrators looking for Conti activity to "scan for unauthorized Atera Agent applications and Any Desk persistence."[6]

Looking Forward into 2022

Dragos assesses with high confidence ransomware will continue to disrupt OT operations, whether through integration of OT kill processes into ransomware strains, flattened networks allowing for ransomware to spread into OT environments, or through precautionary shutdowns of OT environments by operators to prevent ransomware from spreading to OT systems.

Additionally, Dragos assesses with low confidence state-sponsored adversaries may leverage ransomware to mask alternate operations, including theft of intellectual property (including key OT schematic details), reconnaissance of target networks, and other Stage 1 components of the ICS Cyber Kill Chain.

Finally, Dragos assesses with moderate confidence ransomware actors will continue to leverage extortion techniques in pursuit of ransom payments; additionally, Dragos assesses with low confidence these methods will grow in severity and intensity as threat actors deploy any available means to collect their ransom.

References:

1 The Rising Threat from LockBit Ransomware – CyberEason
2 LockBit ransomware recruiting insiders to breach corporate networks – Bleeping Computer
3 LockBIT 2.0 Ransomware – Cyble

[4] LockBit ransomware now encrypts Windows domains using group policies – Bleeping Computer

[5] Conti Ransomware — CISA

[6] Angry Affiliate Leaks Conti Ransomware Gang Playbook – Threatpost