GOLD ULRICK Leaks Reveal Organizational Structure and Relationships

secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

Counter Threat Unit Research Team

Since February 27, 2022, the Twitter @ContiLeaks account and other online personas have been leaking communications containing details about threat actors and their operations. The leaks include more than 160,000 messages exchanged among nearly 500 threat actors between January 2020 and March 2022. The messages reveal close relationships among

multiple threat groups and details about the GOLD ULRICK and GOLD BLACKBURN threat groups' operations. Leaked source code and tool repositories offer unprecedented insights into previously unknown threat actors.

Secureworks® Counter Threat Unit™ (CTU) researchers have historically linked most of the activity referenced in the leaked data to two disparate but highly integrated threat groups:

- GOLD BLACKBURN - This financially motivated cybercrime group has been active since June 2014. The threat actors authored and operated the TrickBot malware from late 2016 until March 2022 and have also distributed malware such as BazarLoader, Anchor, Zloader, and Buer Loader.
- GOLD ULRICK - This financially motivated cybercrime group active has been active since mid-2018. It focuses exclusively on organization-wide ransomware attacks. The group distributed the Ryuk ransomware from August 2018 until early 2021 and has distributed the Conti ransomware since early 2020.

In GOLD ULRICK incidents analyzed by CTU™ researchers, the initial access vector used to distribute the Ryuk and Conti ransomware was usually TrickBot, BazarLoader, or another GOLD BLACKBURN malware payload. The PowerShell Empire and Cobalt Strike Beacon command and control (C2) servers used in these attacks were frequently shared by TrickBot, indicating that a single entity maintained infrastructure for both threat groups. However, other threat groups have used TrickBot to distribute ransomware such as RansomExx (also known as 777), Maze, and LockBit.

The leaked messages reveal that the 'Stern' persona is a leader who makes key organizational decisions, distributes payroll, manages crises, and interacts with other threat groups (see Figure 1). Stern's purview includes all aspects of ransomware distribution as well as TrickBot and BazarLoader operation. This relationship suggests that Stern has a leadership role in both GOLD BLACKBURN and GOLD ULRICK. The messages also include individuals representing GOLD CRESTWOOD (Emotet), GOLD MYSTIC (LockBit), and GOLD SWATHMORE (IcedID), who frequently communicate with Stern and other GOLD ULRICK and GOLD BLACKBURN members. Despite the connection to multiple groups, CTU analysis does not suggest that Stern leads all of these groups.

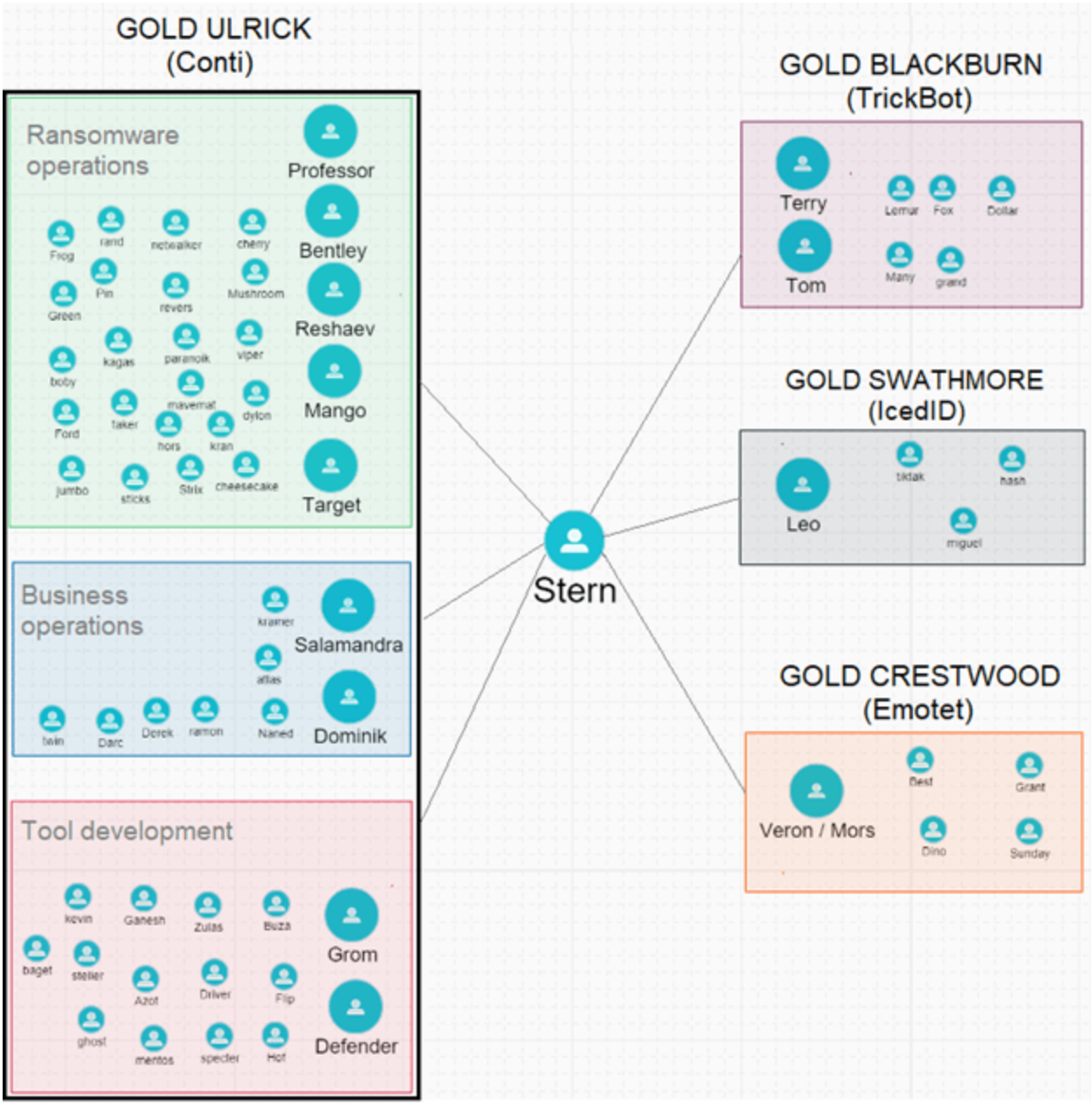

Figure 1. Personas involved in leaked messages, organized by possible organizational structure based on communications. (Source: Secureworks)

The chats reveal a mature cybercrime ecosystem across multiple threat groups with frequent collaboration and support. Members of groups previously believed to be distinct collaborated and frequently communicated with members of other threat groups. This interconnectivity shows these groups' motivations and relationships. It highlights their resourcefulness and ability to leverage subject matter expertise within the groups.

A June 29, 2021 message from the 'Mango' persona to Stern highlights the groups' biweekly salary breakdown (see Figure 2). It describes an operation with 81 people. The average salary per individual is approximately $1,800 USD per month, exceeding the average Russian salary of approximately $540 USD per month. As of July 1, 2021, the Bitcoin address at the bottom of the message had received 2.31 bitcoins (approximately $80,000 USD at that time).

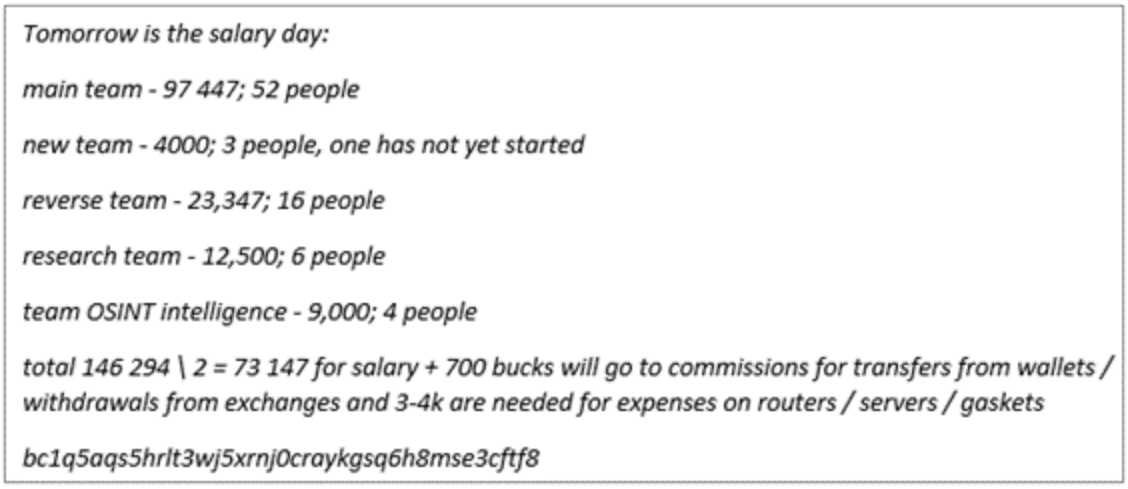

Figure 2. Payroll message from Mango persona to group leader Stern (translated from Russian). (Source: Secureworks)

Other leaked data included more than a dozen dossiers of threat actors with photos, names, addresses, phone numbers, bank account numbers, passport, and citizenship information. The identity and motives of the individual who leaked these dossiers are unknown, so CTU researchers cannot determine if the data is reliable or if it was modified before release. The individual expressed anger toward Russia, so the leaks could be in response to pro-Russian statements GOLD ULRICK posted on its leak site.

As of March 6, 2022, GOLD ULRICK was posting new victims to its leak site. The group's attacks have impacted hundreds of victims and include many high-profile attacks. The exposure from the leaked data could cause the group to cease operation, or could be another obstacle for the threat actors to overcome.

Threat Intelligence Executive Report, Vol 2022, No. 2

Get the latest Threat Intelligence Executive Report from the Secureworks Counter Threat Unit™

Read Now