DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors

mandiant.com/resources/how-mandiant-tracks-uncategorized-threat-actors

Many people are hearing the term UNC for the first time after we published details of a threat group we refer to as UNC2452. “UNC” groups—or “uncategorized” groups—are raw attribution analysis that we previously kept primarily in house. We recently began rolling out UNC information to Mandiant Advantage customers because we want to give users direct access to source materials and raw analysis that Mandiant experts use to write intelligence, respond to breaches, and defend our clients. In light of recent events, we want to provide some more details to the greater public on the UNC designation.

What is an UNC?

An UNC group is a cluster of cyber intrusion activity—which includes observable artifacts such as adversary infrastructure, tools, and tradecraft—that we are not yet ready to give a classification such as APT or FIN. UNCs are created based on a defining, anchoring characteristic often discovered during a single incident. As we discover new artifacts associated with other incidents and proactive collections efforts, the UNC provides a framework to join discrete pieces of evidence together. These clusters can grow, merge with, or break off from other clusters, potentially become combined under a TEMP name, such as TEMP.Warlock, and/or 'graduate' into fully defined groups, such as FIN11, as depicted in Figure 1. In exposing UNC groups in Mandiant Advantage, we are providing a way for users to track the groups that might become APT and FIN groups *before* they 'graduate' into fully defined threat groups and are announced publicly.

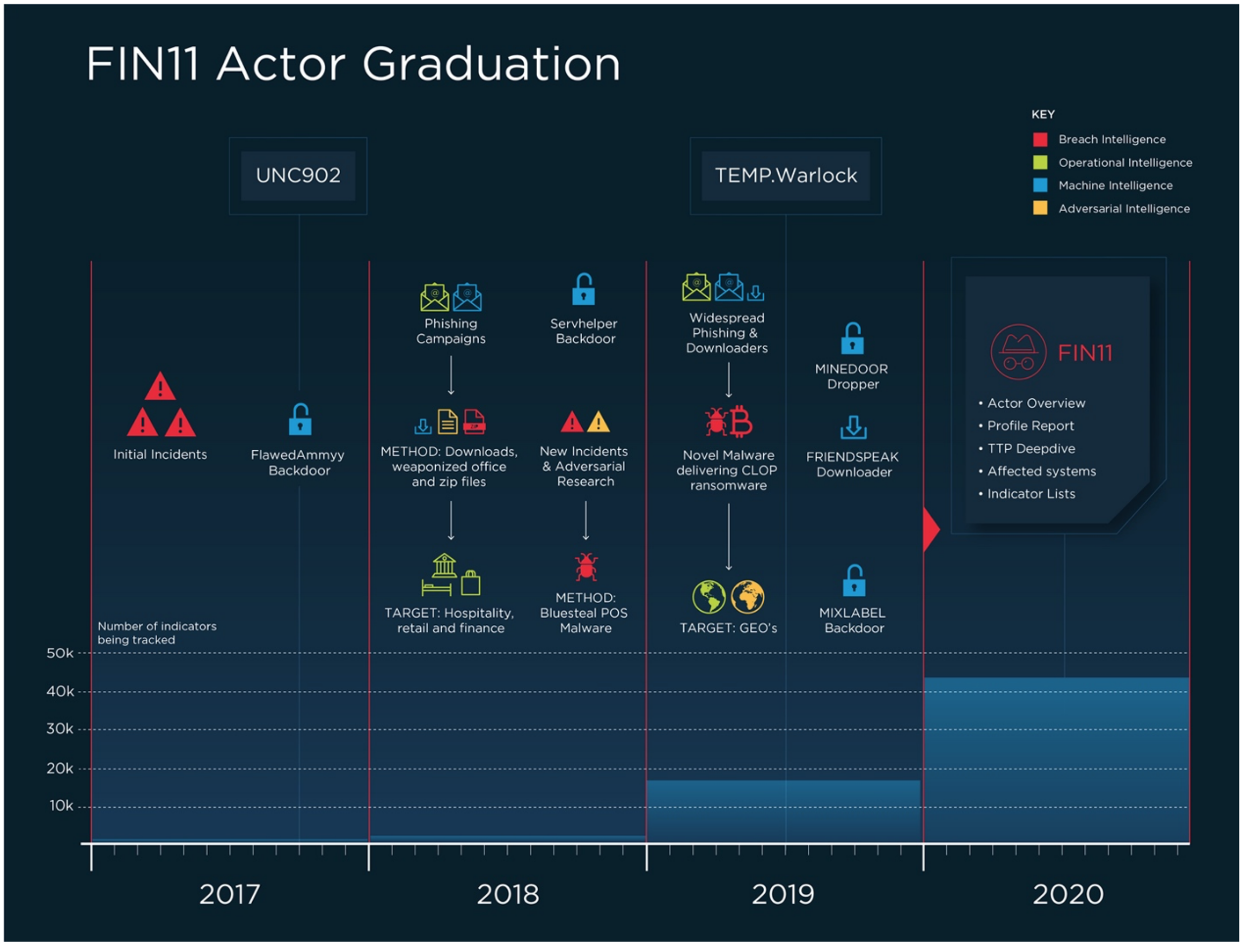


Figure 1: UNC902 to FIN11

Why UNCs Matter

It is important to note that UNCs can undergo significant changes over time based on our evolving understanding of old and new evidence. UNC churn can get messy, that's why we consider UNCs to reflect raw to maturing stages in the attribution process. The road from an initial UNC to an APT or a FIN group typically takes years of painstaking collections, research, and analysis; thousands of pieces of evidence; hundreds of hours of work. But it is worth it! We strongly believe that attribution analysis, as it grows and matures, generates compounding returns for network defenders, equipping them to classify and prioritize response and remediation efforts, as well as predict and prevent some attacks, see Table 1. Even at early phases, UNCs can provide powerful intelligence value.

	UNC characteristics	**Intelligence value**
Tactical	Indicators such as malware, domains, IPs, CVEs exploited	Block lists, detections signatures, patching priorities

Operational	Patterns in behavior, for example frequency of operations, commonly used tools, target locations and sectors	Establish monitoring and mitigations for known TTPs, identify new infrastructure registration or other patterns attempt to predict activity
Strategic	Motives, goals; Potential sponsors, associates	Work the threat group into organizational risk assessment. Consider which threat actors are most likely to affect my organization and why, identify worst-case scenarios from a compromise.

Table 1: Intelligence value of attribution at various stages

How to Use UNCs: Case Studies

UNC1878

We first discussed UNC1878 publicly in March 2020, describing how an initial TrickBot compromise fairly quickly led to the installation of an interactive backdoor and lateral movement. This incident was detected and contained before additional attacker actions were observed, but nonetheless, it fueled additional research and allowed us to link a later compromise where RYUK ransomware was deployed to the original activity set. At that time, the intelligence value was underscoring that widely distributed malware such as TrickBot can be a precursor to a ransomware infection, and the remarkable speed with which UNC1878 in particular progressed from initial foothold to lateral movement—important operational and strategic insights for alert prioritization and risk assessment.

By late October 2020, further research into this activity set uncovered additional malware families and infrastructure as well as a much more robust understanding of the group's most common tactics, techniques, and procedures (TTPs), including how these have both evolved over time. We were also able to identify targeting victimology patterns that allowed us to issue a warning: despite a global pandemic, UNC1878 is actively targeting healthcare facilities with ransomware.

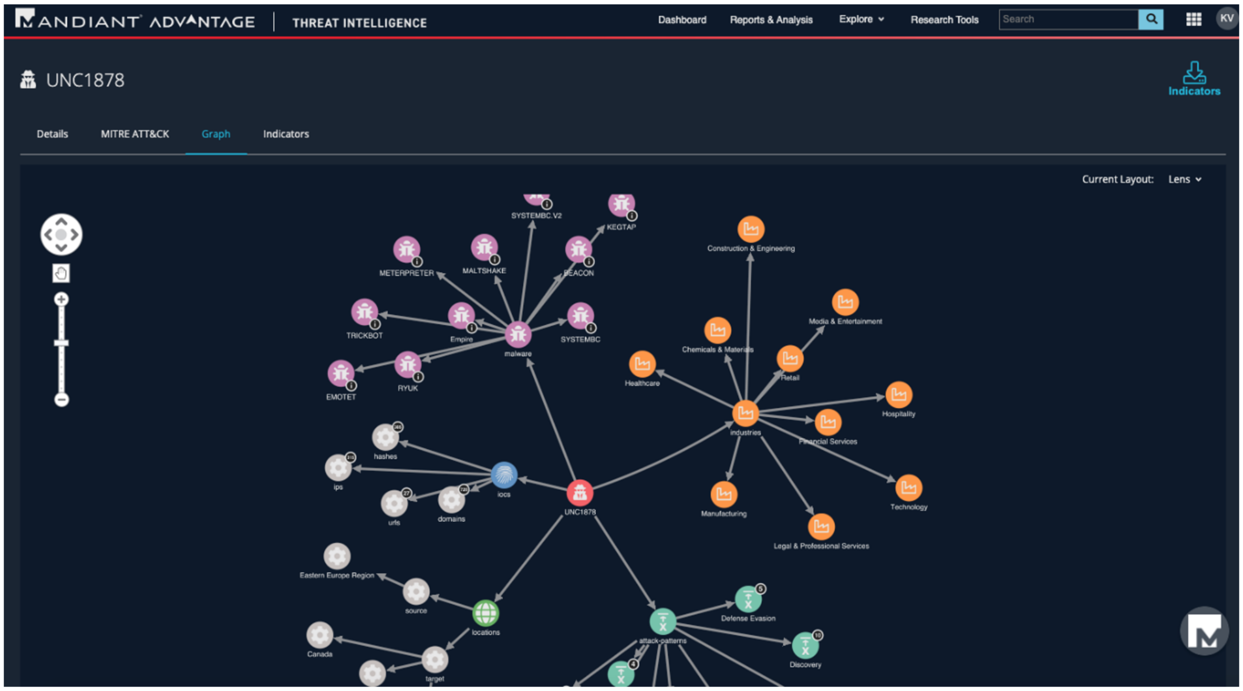
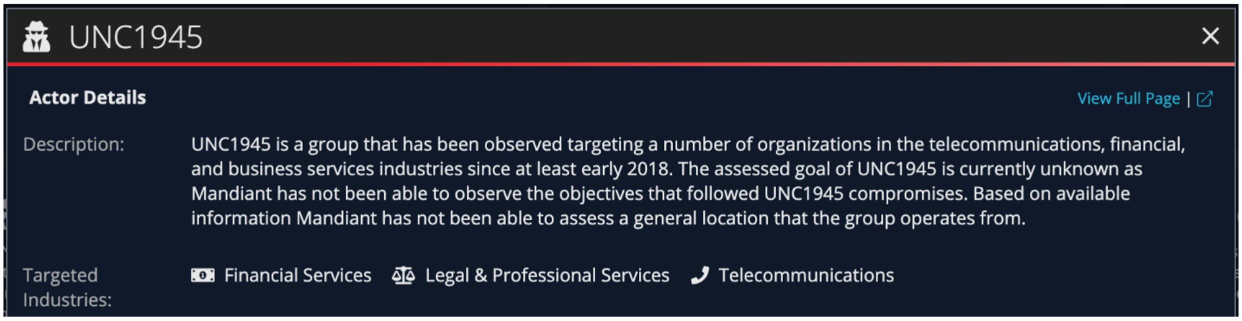


Figure 2: UNC1878 in Mandiant Advantage

UNC1945

UNC1945 represents a case in which we have not yet determined the goal of the attacker, nor information about its potential origin, but the tactics of this activity cluster are significant enough that it is worth calling attention to it. For example, Mandiant discovered UNC1945 exploiting a zero-day vulnerability in the Oracle Solaris Pluggable Authentication Module (PAM), CVE-2020-14871. We reported the vulnerability to the vendor, who recently released a patch. We observed this actor exploit various operating systems and demonstrate access to resources and numerous toolsets as well as traverse multiple third-party networks, suggesting a sophisticated and persistent adversary. We noted that UNC1945 appeared to be targeting specific financial and consulting organizations via third party compromise.

These assessments allow clients to gauge potential strategic risk to their organization based on observed targeting patterns, review tactical strategies for countering third party compromise vectors, as well as download indicators and signatures to take operational defensive steps against this threat.



UNC1945 ✕

Actor Details View Full Page |

Description: UNC1945 is a group that has been observed targeting a number of organizations in the telecommunications, financial, and business services industries since at least early 2018. The assessed goal of UNC1945 is currently unknown as Mandiant has not been able to observe the objectives that followed UNC1945 compromises. Based on available information Mandiant has not been able to assess a general location that the group operates from.

Targeted Industries: Financial Services ⚖ Legal & Professional Services ☎ Telecommunications

Figure 3: UNC1945 actor details

Conclusion

UNC groups support Mandiant incident responders, researchers, and analysts to track malicious activity and turn observations into action to empower defenders. They also represent one way in which Mandiant Advantage is equipping clients to use source materials and raw analysis to improve tradecraft, and hopefully, defensive outcomes in their own environments. Moreover, UNC groups empower users to track activity sets that will become APT and FIN groups before they 'graduate' into fully defined threat groups and are announced publicly—in some cases, years before.