Let’s face it. Sometimes, even the most experienced and capable internal security teams need help in fully determining activity to remove attackers from their environment.

FireEye Managed Defense analysts serve as an extension of a security team, allowing organizations to easily add hundreds of expert analysts with industry recognized cyber security expertise.

This includes frontline experience that leverages +100K hours of IR experience per year from the most impactful breaches.

In a recent incident, Managed Defense live response analysts were engaged by a pretty capable and mature internal security team to help fully scope activity from an attack group that infiltrated their defenses using legitimate credentials obtained in a previous breach in which the client failed to remediate with MD recommendations.

**Backdoor Credentials**

**FIREEYE MANAGED DEFENSE IN ACTION**

**PROBLEM:**
Client breached again via attacker using legitimate credentials obtained from previous attack to gain access via VPN.

**HOW WE DID IT:**
Analysts worldwide actively investigated Live Response endpoint data to observe and fully understand attacker behavior to completely expel the attacker.

**HOW WE DID IT BETTER:**
Through observation and upon attribution of this activity by our Intel analysts, we gained valuable context into the people who were coordinating and taking part in this attack. Based on prior frontline experience and our knowledge of this particular threat actor, we provided remediation recommendations to our client and created new detections based on the activity seen for all FireEye customers.

**RESULT:**
At the end of it all, we were able to identify all parts of the attacker lifecycle, the compromise had been fully contained and the attackers had been fully kicked out of the environment.
Managed Defense analysts utilize behavioral insight into how attackers operate – the tactics, tools, and procedures they use and how they evolve their methods over time – which enables our analysts to quickly ascertain the criticality of a situation, scope the extent of the attacker’s operational capabilities, anticipate their next move, and deliver an effective plan for response.

Because of our experience and knowledge of this particular threat actor, Managed Defense analysts were able to prevent a second full-blown IR investigation and breach that had previously took this client months to investigate and had serious financial impacts.

**Backdoor Credentials**

**BUSINESS IMPACT**

Managed Defense analysts utilize behavioral insight into how attackers operate – the tactics, tools, and procedures they use and how they evolve their methods over time – which enables our analysts to quickly ascertain the criticality of a situation, scope the extent of the attacker’s operational capabilities, anticipate their next move, and deliver an effective plan for response.

Because of our experience and knowledge of this particular threat actor, Managed Defense analysts were able to prevent a second full-blown IR investigation and breach that had previously took this client months to investigate and had serious financial impacts.

**Initial Detection**

- HX Agent detects suspicious activity
- Customer notified of significance of activity
- Client engages FireEye for support
- Performed 4 days of scoping to observe and fully understand attacker activity
- Identified 15+ additional hosts that had been effected
- Collected and analyzed additional data

**Investigation**

- Scoping begins; determine attackers logging in with legitimate credentials via VPN
- FireEye analysts worldwide begin actively investigating live response data and create new detections based on attacker activity
- IR leads join to assist
- Identified all attacker activity and ensured expulsion from entire environment

**Managed Defense Full Scoping and Expulsion**

**56%**

MD customers who were previously Mandiant incident response clients were targets of at least one significant attack in the past 19 months by the same or similarly motivated attack group.*

*2018 Mtrends Report
Backdoor Credentials

**FULL STORY**

In FireEye’s 2018 M trends report, we stated that 56% of FireEye MDR customers who were previously incident response clients were targets of at least one significant attack within 19 months by the same or similarly motivated attack group.

This rang true in one recent engagement, as Managed Defense analysts were called upon to fully scope attacker activity at a client where remediation was not conducted after a previous breach.

As analysts began collecting data to understand the activity, they noticed that 15+ additional systems had been compromised. Upon further analysis, it was determined that the attackers were using legitimate credentials to log in to the clients network via VPN.

Using Endpoint methodology IOCs to detect process executions and NX to identify malware callbacks, MD analysts were able to identify both open source and custom backdoors as well as detect more credential harvesting on additional systems.

Analysts from multiple teams around the world began actively observing and investigating Live Response endpoint data around the clock to gain valuable context into who was coordinating and taking part in the attack while making sure the client was fully protected. Based upon these observations, analysts were able to determine the threat actor and create new detections based upon these observations for not only the client, but all FireEye customers.

After additional scoping and system identification, analysts were able to develop a full understanding of how these attackers were working, managed Defense analysts kicked off a specialized scoping sweep across the client’s entire endpoint fleet to try to identify additional hosts that may not have triggered alerts, which uncovered over 15 additional hosts that had been affected.

In a span of 7 days, MD analysts observed attacker activity to gain a full understanding of who, what, where and why while fully engaging and reporting to the client; intel analysts had fully analyzed the data we obtained and confirmed attribution; and the Malware Reverse Engineering Team had reverse engineered a number of new malware payloads.

At the end of it all, the FireEye Managed Defense Team was able to identify all stages of the attacker lifecycle to fully contain the compromise, kick the attackers out of the environment, and create product detections to protect all FireEye customers.

In FireEye’s 2018 Mtrends report, we stated that 56% of FireEye MDR customers who were previously incident response clients were targets of at least one significant attack within 19 months by the same or similarly motivated attack group.

About APT35:

APT35 (Newscaster Team) is an Iranian Government-sponsored cyber espionage threat actor that conducts long-term, resource-intensive operations to collect strategic intelligence.

**THREAT TYPE:**

APT35 targets include military, diplomatic, and government personnel from the U.S. and the Middle East, as well as organizations in the media, energy, and defense industrial base (DIB) sectors within those regions.

**CAPABILITY:**

APT35 has historically relied on marginally sophisticated tools during operations, including publicly available webshells and penetration testing tools, suggesting a relatively nascent development capability.