CASE STUDY: OPERATION AURORA

Triumfant has performed extensive research into the behaviors of the recent attack directed at Google called Operation Aurora. This case study provides a detailed description of how Triumfant would detect, analyze and remediate the attack on an endpoint machine running the Triumfant agent.

In the interest of full disclosure, Triumfant had no direct interaction with the attack either directly on Triumfant's own endpoints or indirectly through a Triumfant customer. The analysis is based on detailed information collected through a variety of publically available research performed by reliable sources that performed hands-on analysis of the attack. Based on this research, Triumfant is fully confident that our software would have detected the attack and built a remediation that would have restored the machine to its pre-attack condition.

The Operation Aurora attack falls squarely into one of the classes of attacks that Triumfant excels at detecting: targeted attacks engineered to evade traditional network and endpoint protections. While the actual attack vector used was not exceptionally sophisticated, the attack was created to have a digital signature that would not be detected by antivirus tools. The attack also took steps to protect and obscure itself from detection once it infected a machine. The case study steps through the process in four parts: initial detection, diagnosis, the assimilation of data about the attack into the Triumfant knowledge base, and remediation of the affected machine.

Detection

The malicious code used by Operation Aurora created several service keys during three specific steps: execution of the dropper, the first stage of installation, and the second stage of installation. Some of these keys are subsequently deleted but at least one was persistent. The appearance of one or more of these keys would be interpreted as a marker of potential malicious activity by the Triumfant real-time malware scan and would therefore trigger the detection process.[i]

The first step in the detection process would be a request by the agent to the server requesting permission for the agent to execute a full scan of the machine. The purpose of this scan is to capture all of the changes to that machine since the previous scan results were processed as part of the normal agent/server interaction that occurs every 24 hours. The Triumfant server would respond within seconds, authorizing the scan and throttling up the agent to complete the scan as rapidly as possible, collecting all 200,000 plus attributes in under a minute. The resulting scan would captures the state of the machine immediately after infection, providing the raw material for diagnosis so the analytics could verify the machine is under attack and identify all of the primary and secondary artifacts of the attack.

Diagnosis

The Triumfant server would receive the full scan, recognize that it was executed as a result of suspicious behavior, and immediately compare it to the adaptive reference model (the unique context built by our patented analytics). The result of this comparison would be a set of anomalous files and registry keys. The fact that the files and keys associated with Operation Aurora have random names would guarantee that they would be perceived as anomalous despite the fact that humans might tend to confuse them with legitimate Windows services. Further analysis would then be applied to the anomaly set to identify important characteristics and functional impacts. In this case the salient characteristics are an anomalous service and a number of anomalous system32 files.

The discovery of an anomalous service would cause the Triumfant server to build a probe to be sent to the agent for execution to gather more data to complete the analysis. In this case, the probe would contain a list of all of the anomalous attributes found by the server during its analysis. Such probes leverage a series of correlation functions designed to partition the anomalous attributes associated with an attack into related groups. For Operation Aurora these correlation functions would group all of the anomalous attributes and then perform a risk assessment on this group. In this specific case, this analysis would find that the malicious attack is communicating over the internet.

The cumulative results of the correlation and risk assessment would then be sent back to the Triumfant server. This new information is then processed and classified as an "Anomalous Application" with a complete analysis of the changes that composed the attack. This data would show the full set of changes associated with the attack such as files, registry keys,

processes, ports, services, and event logs that were added, changed, or deleted as part of the attack. The data about the attacks would be posted at the console and the Triumfant server would alert the appropriate personnel based on the established reporting and alert protocols. Personnel could then access the correlated attack information and the corresponding risk assessment who could then take appropriate actions including the ability to save the analysis to readily share the data with CIRT and forensics teams.

Knowledge Base

Triumfant has the ability to save the analysis from any anomalous activity and leverage that data to create what Triumfant calls a Recognition Filter that becomes a permanent part of the knowledge base contained in the adaptive reference model. These Recognition Filters have a number of benefits. First, they provide a very precise mechanism for storing and sharing knowledge about an incident. Second, they allow the system to search for any other instances of that particular condition on other machines. Third, they enable the operator to pre-authorize automatic responses - such as automatic remediation - should that incident be detected in the future.

In the case of Operation Aurora, an analyst could save the analysis and build a filter specifically about this attack. Once built, the filter could be used to check other endpoint machines (the entire population or specified groups) for infection. This mechanism uses acquired knowledge to address broad attacks before they have the chance to spread beyond their initial penetration. These filters are also more resilient than digital signatures because they use wildcarding to continue to detect the attack even as it morphs its basic signature over time to avoid traditional signature based tools.

Remediation

The ability to identify and correlate all of the changes associated with any attack provides a depth of information that enables Triumfant to build a contextual and situational remediation that surgically and reliably removes the components of that attack without reimaging the machine. This remediation is built to exactly match the attributes of the anomalous application, in this case Operation Aurora, on an attribute by attribute basis.

For Operation Aurora, Triumfant would construct a remediation to address all of the changes associated with the attack, restoring the altered attributes to their pre-attack condition. This includes the changes Aurora makes to affected machine's configuration settings to either execute or hide itself. The files added to the machine would be deleted, and any files deleted or corrupted would be remediated using Triumfant's patent pending donor technology.[ii]

Summary

Operation Aurora is illustrative of the targeted and well engineered attacks that characterize the evolving threats businesses and government agencies face daily. Based on the available data regarding Operation Aurora, Triumfant can say with confidence that Resolution Manager would have detected the attack, identified changes associated with the primary and collateral damage done to the affected machines, and used that data to build a remediation to address the specific elements of the attack. Within five minutes of the infection Triumfant would have analyzed the attack and created a remediation to return the machine to its pre-attack condition pending confirmation by the administrator. This ability to detect and remediate the attacks that evade traditional endpoint protections demonstrates the unique capabilities of Triumfant's technology.

---

[i] Triumfant uses two continuous scan cycles. One is a scan for markers of malicious activity that runs approximately every thirty seconds. The second is a continuous scan of every attribute on the machine that identifies and collects changes to those attributes and communicates them to the server on a 24 hour reporting cycle.

[ii] Triumfant leverages the knowledge contained in the adaptive reference model to find another machine that has the proper version of corrupted or missing files – validated to the specific release number and MD5 hash - and uses that machine as a donor to repair the affected machine. This technology is patent pending.