A Flight Recorder for Forensics

June 2017

Lior Frenkel, CEO and Co-Founder
Waterfall Security Solutions LTD.

Targeted Attacks

Cyber attacks only become more sophisticated over time, and current trends in targeted attacks, particularly targeted ransomware, are disturbing. When remediating such attacks, reliable forensics are indispensable; how else can we be assured that we have discovered all compromised equipment, and discerned the original attack path?

For more than a decade, targeted remote attacks have breached countless networks, even heavily-defended ones. A targeted attack is one where our attacker has a specific target in mind - us. The common wisdom of "we need only to be better defended than our neighbor" does not hold for targeted attacks. Such attacks often start with "spear phishing" - well-researched, forged emails that trick us into revealing remote login credentials, or into somehow activating malware. Once our enemy has a foothold on our networks, they seed remote-control malware, create new accounts for themselves, and work deeper into the most-sensitive of our networks until they have reached their goal. Their goal may be sabotage, it may be espionage, or in recent months it may simply be extortion.

Compromised Logs

No matter what the goal, once these attackers control equipment on a network, they cover their tracks, defying most attempts to track them down. They erase the evidence of their attacks in local logs, and even reach across networks to erase log repositories, online backups, and SIEM databases.

Manipulation and deletion of logs makes incident response very difficult. What is the first thing our incident response team does when visiting a potentially compromised site? They start making wholesale copies of log files, intrusion detection system and SIEM databases, and entire hard drives of potentially-compromised equipment. They need to capture enough information to determine, eventually and reliably, which machines are compromised and how the original attack came about. The goal is twofold: to ensure that all traces of the attack are eradicated from compromised hosts and networks, and to "close the door" through which the attackers entered our networks in the first place.

These objectives are difficult or impossible to achieve when logs, SIEM databases and other forensic records have been compromised, leaving only unreliable information to examine. Log records are not better secured than the rest of the network, and the network has been breached. Worse, when investigating a potentially-compromised site, the attack may be on-going. When attackers detect that an investigation has started, they may undertake to actively confuse the investigation. They may tamper with forensic evidence, and may tamper with our first-responder equipment, even as those responders are trying to gather evidence.

Waterfall BlackBox

The new Waterfall "BlackBox" solution uses unidirectional technology to help cyber-event responders both before and during incident investigations. The BlackBox creates an online secure storage for logs and other data. Designed to achieve a task comparable to an aircraft flight recorder or “black box,” which stores flight information to survive a crash, the Waterfall BlackBox stores logs and survives attacks. Using an internal unidirectional gateway, the BlackBox copies forensic records from a monitored network into an isolated, “behind the gateway” repository. Each log entry sent to the BlackBox is stored in the database behind the unidirectional gateway, putting those log entries physically out of reach of the network, and thus out of reach of the attackers. The repository can be accessed only by physically connecting to the BlackBox appliance - a task that remote-control attackers are physically unable to undertake.

The BlackBox technology can be used in two modes – pre-emptive and active-investigation deployments.

Pre-Emptive Deployment

When deployed before an attack, the forensic recorder gathers system logs, database snapshots, transaction logs, NetFlow records, configuration files, raw network traffic and other useful forensic data, pre-emptively. The incident response team can then carry out their investigation normally, confident that they have a tamper-proof record of the attack in hand.

This record is useful for post-incident analysis and can be invaluable during the investigation as well. By comparing logs, files and other records to the “BlackBox copy” in real time, the incident response team can quickly learn which records the attackers erased or modified.

Active Investigation Deployment

A portable version of the Waterfall BlackBox is available for sites that may not have deployed the solution pre-emptively. Incident response teams arriving at a site typically deploy the portable BlackBox on a suspect

Copyright © 2017 by Waterfall Security Solutions Ltd. All Rights Reserved.

network as one of their first tasks. Such deployments can serve to capture the details of attacks-in-progress, especially when attackers are actively trying to defeat an investigation in progress.

That the BlackBox uses unidirectional gateway technology under the hood has an additional benefit - first responders can be confident that nothing will leak from the BlackBox back into the monitored network. This is because the BlackBox technology consists of two CPUs separated by the one-way unidirectional gateway hardware, with a large storage array accessible only to the receive-only CPU. The BlackBox storage, behind the unidirectional gateway, is not accessible from any network.

This can be very useful when investigating complex sites with multiple locations and networks, and when comparing records of attacks from multiple sites or even from multiple events. In addition, response teams, especially third-party service providers, can be confident that nothing 'bad' can happen when they move a BlackBox from one site to the other or from one customer to another.

Conclusion

Waterfall's new BlackBox is like a flight recorder for cyber attacks. Real-time, gigabit-speed records can be stored and secured for investigation and analysis, during and after incidents, to provide forensic teams with reliable records of an attack.

About Waterfall

Waterfall Security Solutions is a global leader in industrial cybersecurity technology. Waterfall products, based on Waterfall's innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, offshore platforms, refineries, manufacturing plants, utility companies and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support a wide range of industrial control system and remote monitoring platforms, applications, databases and protocols.

For More Information

Please contact Waterfall directly for additional information on this topic or on any topic related to Waterfall products:

Waterfall Security Solutions
21 Hamelacha, St. Idan Building #2
Rosh Ha'ayin 48091 Israel
info@waterfall-security.com
http://www.waterfall-security.com

Copyright © 2017 by Waterfall Security Solutions Ltd. All Rights Reserved.