Triumfant Whitepaper

Closing the Breach Detection Gap

Overview

The recognition that motivated and sophisticated adversaries are penetrating even the best defenses has been immediately followed by the sobering realization that organizations are not prepared or equipped to detect breaches. A significant gap exists between prevention tools and forensic tools, leaving organizations unable to rapidly detect a breach and provide the actionable information needed to make an equally rapid and well-informed response. Triumfant's unique ability to detect attacks that evade prevention software fills that gap, providing organizations with a rapid detection and response tool to effectively respond to breaches and minimize organizational and reputational risk.

Supporting data for this white paper has been obtained by several studies that are widely regarded in the IT security market, and each is noted in the endnotes. The paper is based on the "presumption of breach" doctrine and does not attempt to establish or debate the probability that a given organization will experience a breach. The wealth of data regarding reported breaches in the cited reports and other credible sources clearly demonstrate that organizations are being breached. Therefore, this paper focuses on the challenges that organizations face when they are breached and a solution for rapidly detecting breaches and creating an appropriate and equally rapid response.

The Breach Detection Gap

You Will be Breached

The number of reported breaches is rising, and the trend shows no sign of slowing. There are several very credible and detailed breach studies available on the market, and the aggregate data from these studies indicates that breaches do not discriminate across organizational size or industry. Furthermore, the targets of many of the highest profile breaches were organizations that carry a presumed high level of technical competence and security acumen. This is a critical point, as organizations cannot afford to adopt a "this won't happen to me" attitude and ignore the evidence.

Figure 1 shows a graphical representation of many of the breaches studied by IBM Security Systems, the breadth of which prompted IBM to declare 2011 the "Year of the Breach".[i]

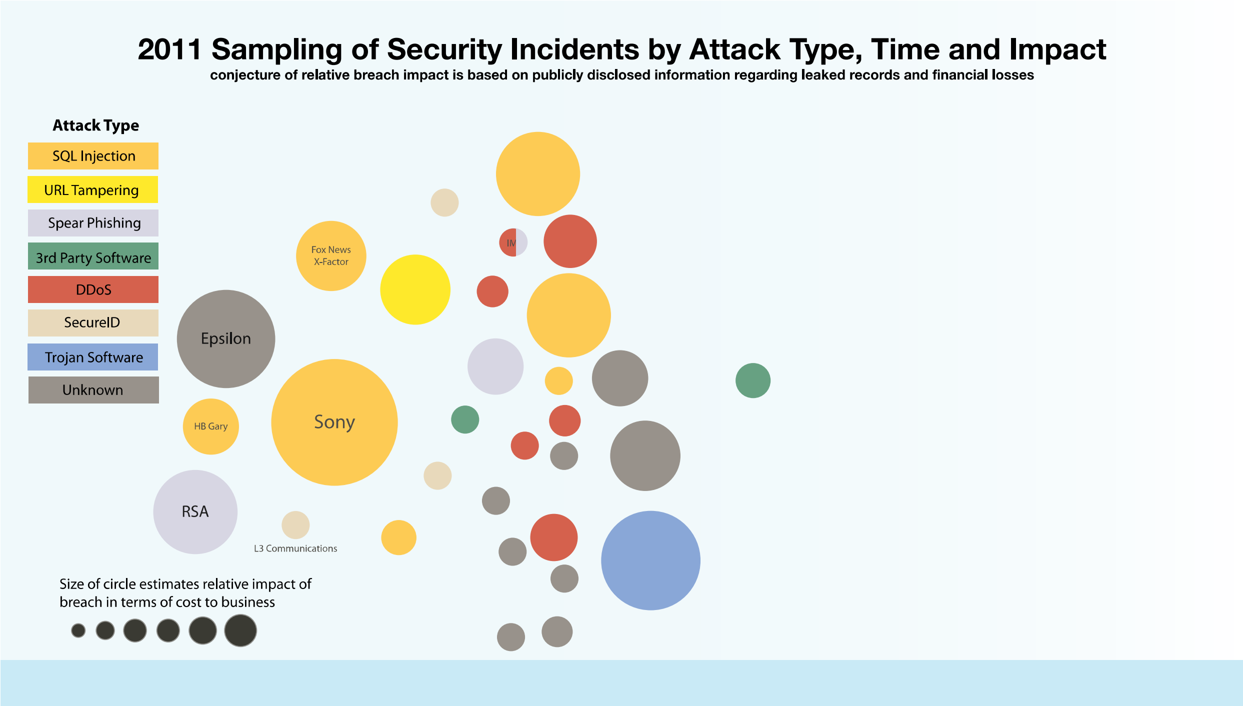


Figure 1: 2011 Sampling of Breaches

Engineering a breach has never been easier. The open market has a wide variety of remote access trojans (RAT) and privilege escalation tools that can be readily utilized, removing technical barriers to entry. In their M-Trends Annual Study, forensic provider Mandiant noted that the adversary used publically available (off the shelf) malware in 77% of the cases they studied.[ii] This demonstrates that attackers can readily evade prevention software even when there is prior knowledge of the malware used in the attack. Second, targeted attacks do not require that the adversary expend huge resources building and employing a zero day attack. Third, the malware often leverages well-known vulnerabilities identified months or years earlier, illustrating that vulnerabilities are quickly exploited, but slowly eliminated. A recent presentation at Shmoocon 2012 demonstrated six methods for evading whitelisting tools, one of the latest silver bullet solutions.

The mounting and clear evidence leaves organizations no choice but to adopt the presumption of breach doctrine: expect that the organization will be breached and be prepared to rapidly detect breaches and launch a timely and informed response.

Defining the Breach Detection Gap

The fundamental realization that motivated and sophisticated adversaries are penetrating even the best defenses brings with it an immediate and daunting question for the vast majority of organizations: am I equipped to detect a breach? The evidence would say no. Consider:

- The Trustwave 2012 Global Security Report noted that the breaches studied in their report remained undetected on the attacked organization's network for an average of 173.5 days[iii]. The Verizon Business 2012 Data Breach Investigations Report (DBIR) notes that 85% of the breaches in their study went undetected for weeks or more, with 55% exceeding 30 days.[iv] These are averages of breaches that were *detected*.
- Of the 850+ breaches investigated in the Verizon Business DBIR, 92% were discovered by a third party - not the affected organization.[v] In the largest organizations that are assumed to be the best equipped for breach detection, only 16% of breaches were detected via active discovery methods.[vi] The numbers indicate that breach detection is left to chance – a customer or partner experiencing anomalous behavior that triggers forensic research.

The inability of organizations to detect breaches is easily explained. As Figure 2 illustrates, between the numerous layers of prevention solutions and forensics tools is a critical gap that leaves organizations unable to detect breaches at the point of infiltration.

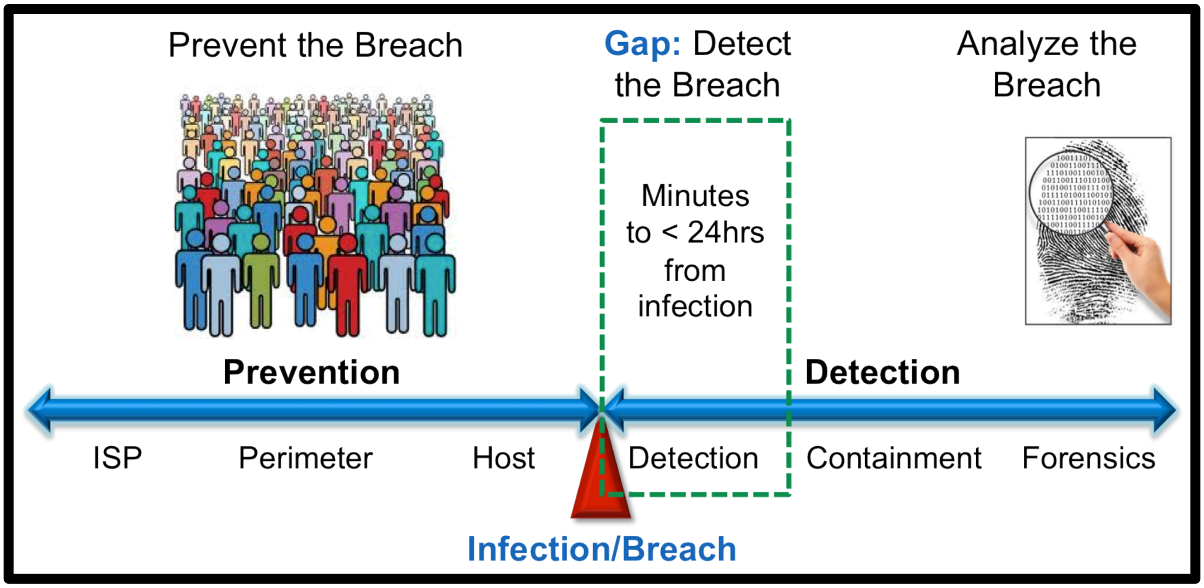


Figure 2. The Breach Detection Gap

Prevention – stopping an attack before it infiltrates the target – has been the focus of the IT security market even though it is abundantly clear that a prevention-centric strategy is doomed to failure. Even as organizations begin to realize that this behavior creates a false sense of protection, the emotional bias toward prevention still drives organizations to push budgets toward the next silver bullet in prevention technologies. Tradecraft relentlessly and rapidly evolves to evade any gains in prevention software, and targeted attacks are engineered to evade the specific defenses meant to defend their target - the malware manifestation of the metaphorical “bullet with your name on it”.

Organizations direct very little budget and resources are toward addressing what happens post-infiltration (breach), and the historical emphasis has been on Forensics tools. These tools provide deep insight and valuable analysis to the breach investigation process, but can only be brought to bear after the breach is detected. Without better detection capabilities, this means that organizations are spending their post-infiltration budget on tools to analyze breaches 173.5 days (on average) after their network has been infiltrated.

The Breach Detection Gap is the critical exposure between prevention tools and forensics tools that leave organizations without the means necessary to detect breaches in real-time. Obviously, without detection there can be no timely response. What organizations need is a tool that detects a breach at the time of infiltration, produces as much forensic information as possible at the time of detection, and provides the ability to take immediate action to stop the attack and repair the machine.

The Consequences of the Gap

The inability of organizations to rapidly and accurately detect breaches effectively plays directly into the hands of today’s adversary that seeks long term, uninterrupted infiltration of key information systems. Smash and grab tactics of the past have been replaced with patience and persistence, with a premium on stealth and long-term access to achieve the goal of the attack. Upon infiltration of a machine, the attacker will take steps to obfuscate any evidence of the attack and their presence on the machine. Attackers often follow a deliberate, patient approach, called “low and slow”, as a purposeful way to complete objectives with minimal risk of exposure. The adversary may have invested significant time and resources building the attack, so they are willing to bide their time to avoid detection.

Some sophisticated attacks have multiple steps, called a kill chain, which each must be executed to achieve the goal. Throughout the process, the attacker is normally able to continuously monitor and control the attack progression, although recent prevention techniques have forced attackers to minimize command and control frequency. The Verizon Business DBIR notes that 71% of the breaches studied had two or more steps and the average breach had nearly three (2.9) phases or steps.[vii]

In some cases, the infiltrated machine is not the ultimate target of the attack, but the first foothold into the network. For example, endpoint machines are used as the pivot point to access server machines where the targeted data or intellectual property resides. In these cases, keyloggers are often installed on the entry point machine to gain the access credentials to move onto other machines. Moving laterally with valid credentials has the added benefit of further shielding the attacker from detection.

Sophisticated threats are engineered to be persistent – the adversary builds mechanisms to restart the attack if discovered and restore command and communication if interrupted. Adversaries gain persistence through many different techniques but the goal is the same: ensure that the attack persists on the machine until the objective is met. A good example is the October 2011 attack on the United States Drone Command and Control Center. Once the attack was identified, the persistence mechanisms introduced on the affected network kept re-infecting the system in spite of significant efforts to remediate the environment.[viii]

The Organizational Risks Created by the Gap

There is nothing positive that comes from having a third party with malicious intent establishing a long-term, clandestine presence on organizational networks. The reason is obvious: persistence and secrecy provides the attacker the time needed to achieve the objective. The resulting risks are many, the consequences are destructive, and the long-term effects can materially impact the organization. Each day the breach remains undiscovered increases the risk to the organization.

Dimensions of Organizational Risk	
Financial	**Reputational**
A report from the Online Trust Alliance says that the average cost of the 558 breaches in their study was $7.2M to the affected organization.[ix] In the 10Q filed on August 5, 2011 by the parent company of RSA, EMC noted a one-time charge of $66.3M as the cost for the RSA breach that was discovered in March 2011.[x] This breach eventually effected over 700 organizations and reportedly cost the banking industry in excess of $100M.[xi] Reported costs to Sony for their repeated breaches have ranged up to $1B.	No company wants to end up on the front page of the *Wall Street Journal* because of a breach. The reputational impact of breaches can erode customer trust and increases customer churn in business segments where churn is a normal factor. Hard dollars are difficult to measure in regards to reputational costs, but it is safe to conclude that organizations would much prefer to avoid the negative publicity associated with high profile breaches.
Valuation	**Existence**
Financial loss and reputational impact can ultimately effect company valuation. One estimate noted that Sony's security problems had negatively impacted valuation 6%.[xii] In fairness, there is no concrete evidence that breaches have a long-term effect on valuation. For example, Heartland Systems rebounded after a very public breach. Studies have linked short-term cause and effect, and it is certain that companies would prefer to avoid even temporary impacts to valuation.	Several companies paid the ultimate price in 2011, as breaches were the catalyst for the companies actually going out of business. The most visible was the Certificate Authority DigiNotar, who shut down operations in September 2011 after reports that it had been breached.

Table 1: The Dimensions of Organizational Risk

The amount of effort needed to devise an attack, infiltrate a network, and remain undetected is not trivial, so there must be an ultimate objective. The risk and ultimately the consequences to the organization are directly linked to the goal of the attack, which fall into consistent categories:

- Data exfiltration. These attacks seek to exfiltrate data records that hold confidential or sensitive information. In many cases, the data is personally identifiable information (PII) that provides direct or indirect access to bank accounts, credit cards, or other forms of data that can be used for financial gain. Data breaches have a high direct costs because organizations must expend resources to address the effects of the breach to make amends to the affected customers. Disclosure regulations also force organization to disclose breaches when PII is involved, so these breaches tend to be the most public.
- Intellectual Property. The United States House Permanent Select Committee on Intelligence has recently reported that lost IP is costing companies billions in lost development capital and potential revenue. Given that data disclosure laws are focused on personally identifiable data, it is likely that the frequency of these attacks is far greater than publicly reported.
- Data gathering. Building a targeted attack or APT requires intelligence about the target. At the highest level, attacks carried out between nation/states may have access to human gathered intelligence. Given that most malware writers have no availability to human intelligence resources, the adversary has taken to creating attacks that gather the intelligence required to power their ultimate endgame. The recently discovered Duqu attack – the so-called "son of Stuxnet" – is a highly sophisticated example of this class of attacks. These attacks use techniques like keylogging to collect the information needed to access highly protected systems and machines.
- Industrial Espionage. The most riveting aspect of the Stuxnet attack was its ultimate goal: an attack on industrial control equipment. Stuxnet effectively disabled laboratory centrifuges in the Iranian nuclear program by causing control equipment to spin the machines at rates above their normal operating profile, ultimately causing damage to the equipment that rendered them unusable. Stuxnet is an extreme example, as it was clearly an extremely sophisticated APT carried out by a nation/state. Given that so much industrial processes are connected to, and run by, industrial control systems it is likely a view into the future.

The evidence would indicate that organizations choosing to ignore the Breach Detection Gap are clearly taking a calculated risk that result in material consequences. At the very least, organizations should consider that the practice of continuing to pour money into prevention tools is yielding diminishing returns, and redirecting some of their budget and resources toward breach detection and response is a prudent shift in priorities.

Rapid Detection and Response

Rapid Detection

Organizations are getting breached, they are not equipped to detect and respond to those breaches, and there are tangible effects on the affected organizations. Better detection is only a partial answer as real value comes from being able to make an equally rapid and informed response to the identified breach. What is needed is rapid detection and response to fully close the breach detection gap.

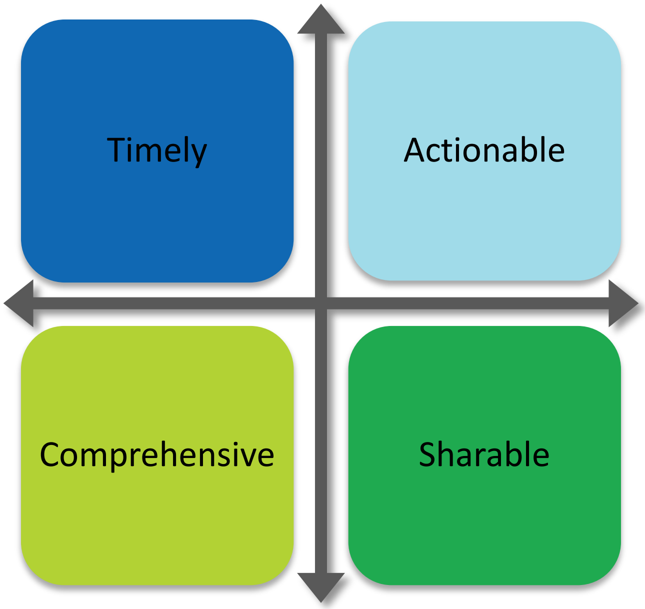
Rapid detection enables the attacked organization to detect multi-phase attacks during the early phases. This early detection hopefully enables the organization to interrupt the kill chain as early as possible with the intent of stopping the chain before data is exfiltrated or other damage is done. As previously mentioned, many attacks have an early phase that uses a keylogger on the endpoint machine for the purposes of providing the adversary the credentials needed to access the server that hosts the targeted data or intellectual property. The ability to detect the early phase attack on the endpoint machine and interrupt the kill chain enables the organization to end the infiltration before the adversary can make the jump from the endpoint entry point.

Beat the Clock

The Verizon Business DBIR indicates that 60% of breaches take a week or more to contain, with less than 10% reaching containment in less than 24 hours. In contrast, 60% of the breaches show that data exfiltration begins in the first 24 hours after the infiltration.[1]

Rapid Response

A rapid response to a breach is clearly advantageous, but empowering a rapid response requires information that shares several essential characteristics:



Speed is not the only dimension that counts in Rapid Response

- Timely. The obvious point is that the quicker the organization gets information about a breach, the sooner it can respond. Statistics from the various breach studies indicate that the attacker does not feel a strong sense of urgency given the current breadth of time between infiltration and discovery. Timeliness is valuable because the first moments of the breach before the attacker begins to move laterally and obfuscate their presence is likely the best time to respond.
- Actionable. It is not enough to simply identify the breach. There must be analysis that provides the information needed to take a measured and informed action. The information must be practical and provide as much information as possible to reduce – or potentially, eliminate - the time needed for additional analysis.
- Comprehensive. Attacks often make changes to machines beyond the introduction of the malicious executable and supporting files. Configuration settings may be altered, ports opened, and persistent mechanisms separate from the main attack planted. Without knowing all of the changes – primary and collateral damage – it is impossible to act without leaving the machine vulnerable to subsequent attacks or allowing the persistence mechanisms to restart the attack.
- Shareable. The analysis must be in a format to readily integrate with other information and tools to facilitate broader analysis and power attribution. For example, information about a detected breach might be integrated with data elements like firewall logs into a SIEM/SIM/SEM tool to provide the analysis needed to better defend against similar attacks. For large organizations with distributed administration, information must be shared to other groups and lines of business in the event that an attack has been used against other machines and networks within the organization.

Automating Rapid Response

Responding to a breach depends on the complexity of the attack, the strength of the persistence methods and sensitivity of the network breached and associated target. Obviously, a simple attack is far easier to remediate than a complex attack that generates a wider blast ring of collateral damage. Effectively breach remediation requires that all of the damage be identified and subsequently repaired. Manual remediation is slowed because organizations frequently lack the tools and human resources required to properly and comprehensively identify the damage from an attack. Remediation scripts ultimately fail for this reason, and because of their reliance on prior knowledge in a world where malware morphs by the minute.

For a rapid detection and response solution to eliminate the need to re-image, the solution must be capable of identifying all of the damage to the machine. This includes the collateral damage such as the modification of configuration attributes, corruption of OS system calls, the opening of ports, and the embedding of processes in existing processes. Once all of the changes are identified, the same tool would need to repair these changes - restore configurations, eject processes, close ports, and repair corrupted system calls. Unfortunately it gets more complex, because some attacks corrupt or delete attributes like registry keys or files. Repairing corrupted or deleted attributes requires a method to provide replacements to these attributes without re-installing software or requiring human interaction.

Triumfant Closes the Breach Detection Gap

If someone were to describe the best case scenario for Rapid Breach Detection and Response, the solution would detect malicious attacks without the need for signatures or any other form of prior knowledge in real time, produce a forensic analysis in minutes, and build a remediation that stops each attack and repairs the affected machine without rebooting or re-imaging. The tool would detect, analyze and repair the problem in minutes without interrupting the end user or their work. In fact, the entire process of detection, analysis and repair could happen without the end user ever knowing that it happened. Information would be shared electronically to other systems and the IT security team so that the information gleaned from the attack could be used for attribution and for further analysis for strengthening the organizations shields. That solution is Triumfant.

Within Minutes of the Breach, Triumfant Will:

- Detect the breach in real-time
- Generate an actionable, comprehensive, analysis
- Build a custom remediation to stop the attack and repair the damaged machine

The Triumfant Approach

Triumfant detects breaches by monitoring host machines for changes, and uses patented analytics to correlate and analyze those changes to identify anomalous and malicious activity. This approach enables Triumfant to identify malicious activity without the need for signatures or any form of prior knowledge. Triumfant identifies the constantly evolving attacks that evade traditional protections, effectively closing the gaps left by firewalls, IPS, and antivirus solutions. This includes zero day attacks, rootkits, targeted attacks, the Advanced Persistent Threat (APT), and the work of malicious insiders.

The challenge lies in accurately identifying and assessing anomalous and malicious changes without the false positives that have plagued past attempts at change detection. Where other change detection software analyzes changes only in the context of the attacked machine, Triumfant uniquely analyzes change in the learned context of the host machine population. Triumfant's analytics automatically builds and maintains this context, and then leverages the context to ensure accuracy and effectively eliminate false positives. Triumfant's analytics have been granted four patents to-date, and three of those patents were granted for the ability to accurately identify, correlate, and characterize change.

The ability to identify and correlate all of the changes associated with the attack enables Triumfant to produce comprehensive analysis of the attack within minutes of the infiltration. Triumfant returns a detailed analysis of the risk factors and a recommended response, along with supporting details of every attribute changed on the machine. The analytics provide in minutes what it would take a seasoned analyst hours or days to produce.

With change detection as the foundation, Triumfant is able to take rapid detection and response to the next level by analytically generating a remediation for the problem. Upon detection of an attack, Triumfant leverages the in-depth analysis to build a situational, contextual remediation that surgically addresses the attack and all of the associated collateral damage. The machine goes from infection to remediation in minutes with no requirement to re-image or reboot the machine.

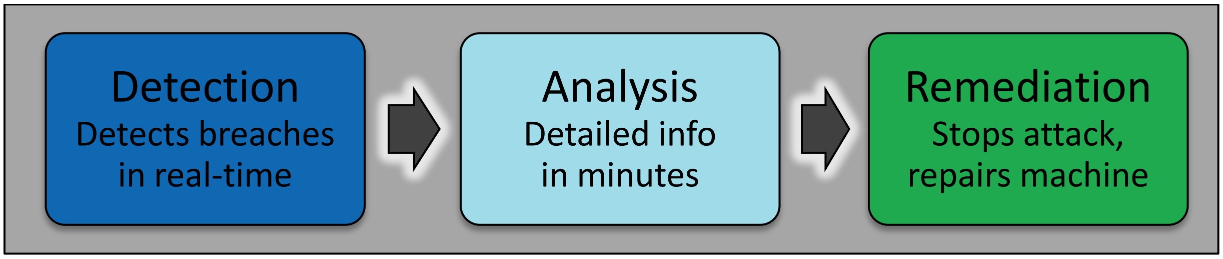

Detection
Detects breaches in real-time
Analysis
Detailed info in minutes
Remediation
Stops attack, repairs machine

Figure 3 - The Components of Rapid Detection and Response

Detection

Triumfant's approach to malware detection effectively closes the breach detection gap, providing rapid breach detection as close to the point of infiltration as possible. Triumfant is built on the premise that to attack a machine you must change the machine, and therefore a solution that detects and analyzes change will see the attacks that evade the protective shields and infiltrate the machine. Of course, the moment an attack infiltrates a machine it becomes a breach. Therefore, Triumfant is at its core a breach detection solution and fills the requirement of rapid detection.

Change detection holds enormous advantage over other detection techniques because it is essentially neutral to attack vector, tradecraft, vulnerability exploited, or delivery mechanism. Eliminating the reliance on prior knowledge enables Triumfant to detect zero day attacks, variations of known attacks, targeted attacks, and the Advanced Persistent Threat – whatever the source of the breach. This makes Triumfant remarkably resilient as the IT security market rides the never ending waves of new attacks and the new silver bullet prevention technologies that are quickly evaded.

For sophisticated attacks that use a kill chain of multiple attack phases, Triumfant will enable organizations to detect the early phases and enable early interruption of the chain to minimize the attack's impact. Triumfant often sees low and slow attacks while they are still dormant by detecting the anomalous files on the affected machine before they actually execute.

Analysis

Creating comprehensive and actionable information about a detected breach is also inherent to the Triumfant approach. That is because Triumfant's analytics are designed to identify, correlate, and analyze all of the changes associated with the attack to provide the data necessary to assess the risk and identify malicious activity. Information is essential to the Triumfant process, not a by-product.

Within minutes of the infiltration, the appropriate personnel have actionable information in their hands, empowering them to assess the situation and construct a timely response. There is a summary overview that contains a description and recommendation, as well as the identified risk factors. The summary also includes information about related processes and executables, high frequency strings, and associated Internet connections. The analysis then provides detail on every affected attribute including registry keys, files, ports, processes, and services. It is possible to drill into the detail for each attribute to see exactly what changed and how it changed. No other tool provides the breadth and detail produced by Triumfant for each detected breach.

The analysis can be surfaced in a variety of forms and integrated directly into other tools. The detailed information about the breach is easily forwarded for further analysis by the incident response team or the forensics team. Triumfant will generate a syslog in the ArcSight Common Event Format (CEF) for integration into SIEM tools to correlate information about the breach with firewall logs and other data. The information can be imported into a wizard for the construction of Triumfant filters that can be used to search for the attack on other machines and networks.

Response (Remediation)

Triumfant's comprehensive analytics enables Triumfant to build a definitive and timely response to breaches by using the detailed information assimilated by the analytics to construct a remediation specific to the detected breach. The remediation is surgically precise, constructed to stop the attack and remove the undesirable collateral damage. Open ports are closed, modified configuration settings are restored, corrupted or deleted files are replaced, and registry entries are repaired.

The remediation repairs the machine while in operation, eliminating the need to reboot and or any other interruption in service. The defense industry calls this "fighting through" – attacks on machines are detected and repaired with minimal (near-zero) impact on the mission. The remediation is not a rollback or a reset to a captured image – it is a surgical repair of the attributes affected by the attack. Consequently, the user of the host machine will not lose any of the desired changes in the process. It is entirely possible that the user may have their machine attacked and subsequently repaired by Triumfant without the user knowing it happened. Triumfant can detect an attack, perform the analysis, and remediate the machine in minutes. It is reasonable to claim that Triumfant could complete the entire detection, analysis and remediation process in less time than it takes to initiate the manual process of alerting an analyst and beginning the first steps of collecting data about the malicious activity.

Remediating malware is more difficult than simply deleting the associated files and registry. Addressing missing or corrupted attributes requires restoring those attributes. Triumfant unique "Donor Technology" leverages the learned context of the host machine population to turn the population into a donor base to fix missing or corrupted attributes, including files and registry keys. For each missing or corrupted attribute, Triumfant interrogates the learned context to find a list of candidate donor machines that have the attribute required to repair the affected machine. The analytics verify the integrity of the donated attribute, which is then used to repair the corrupted attribute. Donor Technology is a unique innovation of Triumfant and is the subject of Triumfant's fourth patent.

For a detailed explanation of how Triumfant detects and remediates malware, please refer to the Triumfant White Paper Detecting and Remediating Malicious Attacks.

Benefits

Triumfant's unique and innovative approach to Rapid Detection and Response has many benefits:

- Triumfant emphatically closes the breach detection gap and gives organizations the Rapid Detection and Response tool they need to reduce the risks – financial, reputational, and regulatory - associated with undetected breaches.
- No tool can completely protect an organization from the loss of sensitive data or intellectual property. The real-time detection of breaches by Triumfant increases the probability that IT Security can address a breach before sensitive data or IP is exfiltrated, thereby reducing the risk and subsequent costs to the organization and preventing a potentially material event.
- Triumfant delivers a comprehensive forensic analysis and builds a situational and contextual remediation in minutes. The tasks of performing commensurate analysis and building a remediation would each take an analyst hours or days to produce. By providing both within minutes of the attack, Triumfant empowers the organization to formulate an informed response to any attack and provides the means to stop the attack and repair the machine. Automating the analysis and remediation process allows staff resources formerly consumed by investigating attacks and writing remediations to pro-actively work to prevent attacks rather than react to attacks. This repurposing of critical security staff effectively lowers organizational risk.
- Triumfant builds a remediation that removes the malicious code and all of the changes to the machine associated with the attack. The remediation is complete, repairing the damage to the machine without losing productive changes. There is no interruption of service to the user, and no need to restart the machine. Because the remediation is complete, there is no need to re-image.
- Triumfant is neutral to attack vector, tradecraft, and delivery mechanism. For example, recent attacks have evaded detection by tools such as deep packet inspection solutions buy using portable memory devices (USB sticks) or wireless connections. As malware continues its relentless evolution, Triumfant's approach will continue to detect breaches because of the nature of the Triumfant approach. Triumfant is not a shield, but it does provide organizations ongoing detection coverage for zero days and evolving attacks until preventative technology catches up.
- Triumfant is designed to complement and extend other IT security tools with integrations to AV suites, SIEM tools, and Trouble Ticketing tools as an example. The data captured about the attack and the subsequent remediation is invaluable information for CIRT and forensic teams for use in enhancing organizational defenses and reducing the attack surface.

Conclusion

Organizations are being forced to quickly embrace a new reality: organizations will be breached, organizations are not prepared to detect and respond to being breached, and the adversary is taking advantage of these circumstances. A significant gap exists between prevention tools and forensic tools, leaving organizations unable to rapidly detect a breach and provide the actionable information needed to make a rapid and well-informed response.

Triumfant detects breaches in real-time, generates a comprehensive and actionable analysis with minutes of the attack, and builds a situational remediation that stops the breach and repair all of the primary and collateral damage to the machine. Triumfant effectively and efficiently closes the breach detection gap with one innovative solution and eliminates the associated risks for the organization.

To learn more about the Triumfant solution, please visit the Triumfant Web Site at www.Triumfant.com request additional information via Info@Triumfant.com.

End Notes

[i] Casey, Bryan; et al (March 2012). IBM X-Force 2011 Trend and Risk Report. IBM Corporation. Retrieved from https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report. p. 12.

[ii] M-Trends Report (March 2012). Mandiant Corporation. Retrieved from http://www.mandiant.com/. p. 2.

iii Percoco, Nicholas; et al (February 2012). Trustwave 2012 Global Security Report. Trustwave Corporation. Retrieved from https://www.trustwave.com/global-security-report. p. 10.

[iv] Baker, Wade; et al (March 2012). Verizon Business 2012 Data Breach Investigations Report. Verizon Business. Retrieved from http://www.verizonbusiness.com/Products/security/dbir/. p. 49.

[v] Verizon Business 2012 Data Breach Investigations Report. p. 49.

[vi] Verizon Business 2012 Data Breach Investigations Report. p. 51.

[vii] Verizon Business 2012 Data Breach Investigations Report. p. 57.

[viii] Rashid, Fahmida (October 8, 2011). *eWeek.com*. U.S. Strategic Drone Fleet Infected by Stealthy Keylogger Malware. Retrieved April 17, 2012 from http://www.eweek.com/c/a/Security/US-Strategic-Drone-Fleet-Infected-by-Stealthy-Keylogger-Malware-561651/.

[ix] Online Trust Alliance (January 2012). 2012 Data Protection & Breach Readiness Guide. Retrieved from https://www.otalliance.org/resources/incident/2012DataBreachGuide.pdf. p. 4.

[x] EMC Corporation 10-Q, Quarterly report pursuant to sections 13 or 15(d). Filed on 08/05/2011. Filed Period 06/30/2011

[xi] King, Rachael (June 8, 2011). *Bloomberg.* EMC's RSA Security Breach May Cost Bank Customers $100 Million. Retrieved April 15, 2012, from http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html.

[xii] Osaw, Juryu (May 9, 2011). Wall Street Journal Online. As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill. Retrieved April 15, 2012 from http://online.wsj.com/article/SB10001424052748703859304576307664174667924.html.

Triumfant® leverages patented analytics to detect malicious attacks that evade traditional protection software solutions by discovering, diagnosing, and repairing unwanted changes by building a situational remediation that stops the attack and repairs the collateral damage to the machine. Triumfant uses the same processes and analytics to continuously enforce configurations and policies, ensuring that organizations start every day with their machines audit ready. Triumfant collects and analyzes more state data than any endpoint solution, making Triumfant the most comprehensive source for state data on the market. For more information about Triumfant, visit www.Triumfant.com.