Cyber Threats on a Path to **DESTRUCTION**

How Supervised Machine Learning Gives Cybersecurity Defenders a Fighting Chance

BLUVECTOR®

Contents

Executive Summary 2

What Is ‘Destructive Malware?’ 2

The Malware Development Cycle: From Collaboration to Commodity 4

Destructive Malware: Why Your Current Security Stack Isn’t Enough 6

Supervised Machine Learning: Your Best Defense Against Destructive Malware 7

Conclusion: Stop Destructive Malware Proactively 9

How BluVector’s Supervised Machine Learning Technology Won’t Leave You Sobbing Over WannaCry Variants 9

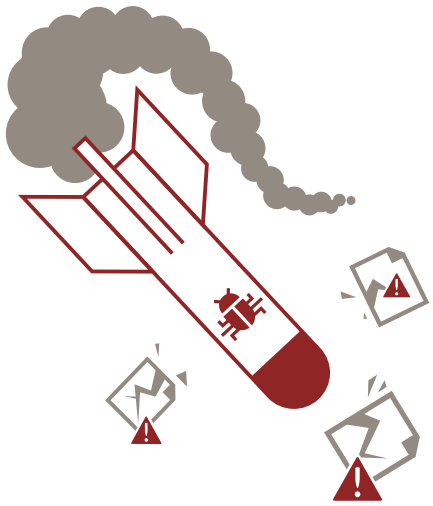
About BluVector 10

Executive Summary

Destructive malware, today's most dangerous form of malware, currently is being used by nation-state actors to destroy computers and disable large networks. As destructive malware becomes commoditized and more accessible to cybercriminals of all stripes—as polymorphic malware and ransomware has—you must be prepared to stop it before your network is destroyed, your data lost or stolen, and your business put at jeopardy.

Read this white paper to learn:

- The definition of "destructive malware" and its salient characteristics;
- The impact of destructive malware and the challenges incident responders face in detecting and remediating it;
- The various tools commonly available to incident responders—and why they fall short against this threat;
- How BluVector's unique supervised machine learning technology identifies and alerts you to the presence of destructive malware before it can wreak havoc on your systems.



What Is 'Destructive Malware?'

Destructive malware. The term sounds redundant, like "serious crisis" or "end result." In fact, it is the latest advancement in malware that takes the already cunning ways in which polymorphic malware enters and hides within your system and melds it with **a payload that will destroy your network *and* data with the precision of a military cruise missile.**

US-CERT (United States Computer Emergency Readiness Team) describes destructive malware as:

> [Having] the capability to target a large scope of systems, and... potentially execute across multiple systems throughout a network. As a result, it is important for an organization to assess their environment for atypical channels for potential malware delivery and/or propagation throughout their systems.[1]

[1] *US-CERT. Security Tip (ST13-003): Handling Destructive Malware. (US-CERT, October 1, 2016)*

Shamoon, the first version of destructive malware that can be broadly applied to civilian environments,[2] was first spotted in the wild in 2012, when nation-state perpetrators, allegedly Iran, destroyed 35,000 Saudi Aramco workstations and put the energy company's supply of 10 percent of the world's oil in jeopardy.[3] US-CERT has specifically described Shamoon as "an information-stealing malware that also includes a destructive module… render[ing] infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable."[4]

Shamoon destroyed 35,000 Saudi Aramco workstations and put **10% of the world's oil** supply in jeopardy.

The original Shamoon malware has three primary functional components that later strains of destructive malware follow as a general template:

Dropper

The origination point of the infection to propagate the malware, it spreads the virus by copying itself onto other computers on a network

Wiper

This module wipes out all data on a computer and makes it inoperable

Reporter

This module reports infection information back to the attacker.[5]

Newer versions of destructive malware provide functional improvements over the original Shamoon malware. Shamoon 2.0, first reported in November 2016, reused 90 percent of the code of the original Shamoon,[6] but it also comes with "a fully functional ransomware module, in addition to its common wiping functionality," and installs a legitimate-looking driver that changes the infected computer's system date to a random one between August 1–20, 2012 to "fool the driver's license checks and evaluation period."[7]

---

[2] *Stuxnet (2010), arguably the first known version of destructive malware, was built to undermine Iran's nuclear capabilities.*

[3] *Pagliery, Jose. "The Inside Story of the Biggest Hack in History." (CNN Money, August 5, 2015)*

[4] *US-CERT. Joint Security Awareness Report (JSAR-12-241-01B): Shamoon/DistTrack Malware (Update B). (US-CERT, April 18, 2017)*

[5] *Symantec Security Response. "The Shamoon Attacks." (Symantec, August 16, 2012)*

[6] *Samani, Raj & Beek, Christiaan. "Shamoon Returns, Bigger and Badder." (McAfee, April 25, 2017)*

[7] *Kaspersky Lab. From Shamoon to StoneDrill: Wipers Attacking Saudi Organizations and Beyond. (Kaspersky Lab, March 5, 2017), 12*

StoneDrill, another type of destructive malware that was discovered around the same time as Shamoon 2.0, stylistically is similar to Shamoon 2.0, particularly its "heavy use of anti-emulation techniques in the malware, which prevents the automated analysis by emulators or sandboxes."[8] However, StoneDrill's code is different, and it has even more dangerous properties than Shamoon 2.0, including:

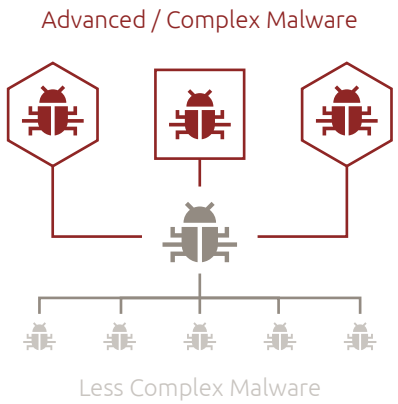
- A disk wiper injected directly into the memory of the user's preferred browser, rather than through drivers;
- More advanced anti-emulation techniques;
- External VBS scripts to run self-delete scripts.[9]

According to Kaspersky Lab, StoneDrill has attacked several energy targets in Saudi Arabia and one target in Europe, but information about its impact on these targets has yet to be made public.[10] The Shamoon 2.0 campaigns have reportedly broadened their scope to target other parts of Saudi Arabia's infrastructure, including financial services and the public sector along with the energy sector. The scale of the campaign, which comprise multiple waves of attacks, suggested that it was the comprehensive operation of a nation-state that disrupted another nation using a coordinated attack.[11]

The Malware Development Cycle: From Collaboration to Commodity

The complexity and collaboration aspects of destructive malware, combined with the large-scale targets that were singled out by hacktivists for its use, suggests that this latest advancement in malware is not an immediate concern for most organizations. But that assumption is foolhardy at best.

If nothing else, the last five years have shown that as malware evolves into more advanced and complex configurations, comparatively less complex types of malware trickle down for use by other criminal elements, typically for monetary gain or the theft of sensitive data or intellectual property. Cybersecurity consulting firm Mandiant says that cybercriminals have caught up in sophistication to the types of attacks originally used by nation-state attackers to the point that the line "between the level of sophistication of certain financial attackers is not just blurred—it no longer exists,"[12] although nation-state attackers "will continue to set the bar for capabilities and sophistication."[13]



[8] *Kaspersky Lab, 14.*
[9] *Kaspersky Lab, 24.*
[10] *Raiu, Coston; Hasbini, Mohamad Amin; Belov, Sergey; Mineev, Sergey. "From Shamoon to StoneDrill: Wipers Attacking Saudi Organizations (blog post infographic)." (Securelist, March 6, 2017)*
[11] *Samani & Beek*
[12] *Mandiant. M-Trends 2017: A View From the Front Lines. (Mandiant, March 2017), 9*
[13] *Mandiant, 9.*

In a recent statement, U.S. Director of National Intelligence Dan Coats concurred:

> Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years … Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies.[14]

As the profit potential of a given type of malware becomes obvious, nation-states and other large cybercrime groups frequently collaborate to develop more sophisticated versions of a given type of malware that benefits the aims of both groups.[15] The Moore's Law-style pace of ransomware development over the last five years is a testament to this. A recent United States interagency government technical guidance document reports that ransomware has become "a growing criminal activity involving numerous variants... [which] have become more sophisticated and destructive."[15] More recent variants can encrypt the contents of networked drives, externally attached storage drives and cloud storage services "that are mapped to infected computers."[16] As discussed in the previous section, the improvements in Shamoon 2.0 and StoneDrill code over the original Shamoon attests to this ongoing progress and advancement.

As a given style of malware becomes more commonplace, collaboration gives way to competition and commoditization. Ransomware, once the province of sophisticated threat actors, is easily available on the darknet. For just $39 on the darknet, code-illiterate criminals can buy a Stampado Ransomware lifetime license that includes technical support.[17] Cerber Ransomware uses a "ransomware-as-a-service" model where the criminals take a 40-percent cut in any earnings Cerber brings to a customer,[18] suggesting the potential for lucrative passive income streams among the criminal underground.

As malware becomes commoditized, prices drop. GM Bot, a strain of Android mobile banking malware, sold for $15,000 in March 2016. Soon, competing strains KNL Bot and Bilal Bot came out with competing malware that sold in the $3,000–$6,000 price range. KNL Bot offered similar features to GM Bot at a lower price point than the latter, while Bilal Bot sold for around $3,000, a price that included unlimited bug fixes and a simpler feature set, that its authors claim was less likely to crash or be discovered.[20]

---

[14] *Coats, Dan. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee. (Office of the Director of National Intelligence, May 23, 2017), 1*

[15] *Higgins, Kelly Jackson. "Ex-CIA Director Brennan Warns of More Collaboration Between Nation-States and Cybercriminals." (DarkReading, June 14, 2017).*

[16] *United States Department of Justice. How to Protect Your Networks from Ransomware. (U.S. Department of Justice, 2016), 6*

[17] *DOJ, 6*

[18] *Beale, John. "The Market of Malware: Buying, Selling and Collaborating in the Criminal Underground." (Security Alliance, Oct. 28, 2016)*

[19] *Ibid*

[20] *Kessem, Limor. "Mobile Malware Competition Rises in Underground Markets." (Security Intelligence, April 28, 2016)*

Given the increased competition for malware revenues, cybercrime organizations, like most thriving businesses, will push innovation in the hopes of greater profits and market share—and destructive malware is just the latest advance in the malware development cycle, soon to be at a darknet near you.

Destructive Malware: Why Your Current Security Stack Isn't Enough

Most organizations have implemented a layered, defense-in-depth security approach that encompasses signature-based anti-virus, sandboxes, endpoint protection and network anomaly detection. But *none* of these solutions are enough to detect, let alone act on, destructive malware like Shamoon 2.0 or StoneDrill before either has wreaked havoc. Anti-virus software (which has had limited value at best for most of today's malware) is based on hindsight. It needs to compare unique, brittle and threat-specific signatures to known malware or viruses, which is useless against often basic variations of known malware, let alone against polymorphic malware that can change code and byte sequences autonomously.

Sandboxes were useful in stopping later Shamoon 1.0 attacks, but newer versions of destructive malware, Shamoon 2.0 and more notably StoneDrill, has been engineered with advanced anti-emulation techniques that allow it to elude virtual machines (VMs) and sandbox detection.[21] Moreover, sandboxes lack the capabilities to analyze large volumes of data because of a limitation on computing power. Commercial sandboxes are forced to select and scan a small subset of content relying on basic signatures, rules, heuristics or random sampling to maintain a reasonable volume, letting malware easily slip through.

[21] *Kaspersky Lab, 24.*

The Path to Destruction

Since the 1980s, new trends have emerged in the threat landscape, as malicious actors develop new tactics and techniques to attack their targets. While the motivations have varied over time, the overall impact of these innovations have increasingly become more severe. The year 2012 marks the beginning of new types of malware that have forced dramatic changes in defenses and behaviors across the cybersecurity industry.

- 1982 — Logic Bomb
- 1983 — Trojan Horse
- 1984 — Phreakers
- 1987 — Worm *e.g. Morris Worm '88*
- 1989 — Cyber Espionage *e.g. AIDS Virus*, Hacktivism *e.g. WANK worm*
- 1990 — Rootkits, Viruses *e.g. ILOVEYOU*
- 1992 — Polymorphic Malware
- 1994 — Mass SPAM, Script Kiddies, DDoS
- 1995 — Macro Viruses, Spamware
- 1996 — Nation-States *e.g. N. Korea trains 500 hackers* Cryptovirology *Basis for ransomware*
- 1998 — C2 (Command & Control), SQL injection, DNS Hijaking
- 2005 — Botnets, APT
- 2007 — Spear Phishing
- 2010 — Weaponized Malware *e.g. Stuxnet*
- 2011 — Data Breaches *Estimated $2bn in damages*
- 2012 — Ransomware *e.g. Police Locker*, Destructive Malware *e.g. Shamoon*

Examples of a few methods threat actors use to easily evade sandboxes include:

- Cause malware to delay execution in VMs by exceeding their time-out period (commonly set to 15-minutes) to observe for malignant activity;
- Leverage vendor-specific sandbox bypass methods, many of which are available online;
- Require user interaction before launching malware;
- Require target-specific data like a cookie, certification or second file to execute.

More recent security approaches like network behavior anomaly detection (NBAD) and user behavior analytics (UBA) use unsupervised machine learning to gain insight into the behavior of possible malware, seeking unusual patterns for suspicious activity. However, even these technologies are no match for destructive malware. For one thing, both methods tend to be noisy, inundating incident responders with alerts, because they cannot differentiate between anomalous activity that is not necessarily malicious and genuinely malicious activity. Moreover, if malware has infiltrated the network when baselines are being set, it activity may be mistaken as normal.

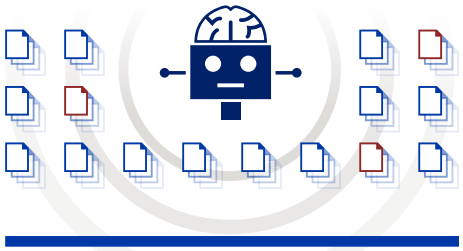
Finally, malware increasingly is being designed to mimic normal behavior to avoid detection and fool unsupervised machine learning technologies. It may lay dormant in a network for days, months or even years before it is activated with catastrophic damage in one fell swoop.

Malware may lay dormant in a network for days, months, or even years before it is activated with catastrophic damage in one fell swoop.

Supervised Machine Learning: Your Best Defense Against Destructive Malware

Supervised machine learning, the latest advancement in malware detection technologies, can identify destructive malware like StoneDrill and Shamoon 2.0, as well as their inevitable variants and unknown threats that have yet to be deployed. Supervised machine learning is used for predicting the classification of unknown data input based on learned features from observing a pre-labeled data set. In cybersecurity, this is akin to a reverse engineer accumulating decades of experience observing the common characteristics that are indicative of both benign and malign files and software.

While traditional approaches such as signatures look for a specific string to determine if a file is malware, supervised machine learning identifies various combinations of characteristics throughout all layers of the content to determine the likelihood of whether that file is indeed malware. This is important for two reasons. First, 70-to-90 percent of malware samples are unique to an organization "from a signature/hash perspective; when compared byte-to-byte with all other known malware, there's no exact match."[22] Second, while malware is often designed to mimic the behavior of safe files, its binary characteristics are unlikely to look normal or safe even if they do not appear malicious. Therefore, analyze *all* aspects of a file for the presence and absence of characteristics to determine whether its various combinations of markers put it higher on the malicious end of a continuum of what is likely to be good and bad.



Supervised machine learning is fast. BluVector's supervised machine learning technology can analyze files and software in milliseconds, right as they enter a network.

Moreover, supervised machine learning is *fast*. BluVector's supervised machine learning technology can analyze files and software in milliseconds, right as they enter a network. Leveraging this technology, BluVector's solution performs high-speed static analysis across hundreds of pieces of content that is reconstructed from millions of packets per second. This capability takes pressure off incident responders, who simply lack the time and bandwidth (as no human could) to determine the potential harm of every file that passes through a network. By using BluVector's algorithm to perform a first pass on the content of all these files, incident responders then can prioritize their time and attention on files that have already been flagged as possible malware.

BluVector further substantiates its findings file and network metadata, along with third-party threat intelligence data, network behavior logs and analysis from integrated tools like sandboxes that would look at behavior. Then BluVector gathers this information for incident responders to remediate directly using complementary tools and through automations. For example, information gathered by BluVector may then be aggregated by an organization's SIEM (Security Information and Event Management).

Finally, BluVector's supervised machine learning algorithm is iterative in nature, enabling it to obtain ever closer approximations of identifiers that would predict whether a file is potentially malicious through additional samples collected within a specific environment. And unlike other security technologies, these supervised machine learning models can be quantitatively measured—so that you can directly verify the improvements.

---

[22] *Verizon. 2015 Data Breach Investigations Report. (Verizon Enterprise Solutions, 2015), 10.*

Conclusion: Stop Destructive Malware Proactively

While destructive malware arguably has the potential to bring about more damage than any malware strain before it, malware in general has placed incident responders at a disadvantage because it has been so hard to discover, let alone stop from unleashing irreparable damage to your organization.

Visibility is "a fundamental capability for any effective security team, and blind spots in the infrastructure can lead to major problems."[23] Without the ability to scan every packet streaming in and out of your network, you lack the threat visibility necessary to protect your organization from cyberattacks and their potential fallout on so many levels.

BluVector has **99-PERCENT ACCURACY** in detecting even the most sinister, protean malware.

The latest advancement in malware identification, supervised machine learning provides you with the power to identify and isolate malware, whether it's basic Stampado ransomware or multifaceted destructive malware like Shamoon 2.0 and StoneDrill. And BluVector's supervised machine learning solution is the only one that can give you 99-percent accuracy in detecting even the most sinister, protean malware that threat actors can create and you otherwise would have never anticipated.

How BluVector's Supervised Machine Learning Technology Won't Leave You Sobbing Over WannaCry Variants

The recent WannaCry ransomware attacks have left organizations reeling. The worry has not been about the damage this particular piece of malware caused (which was minimal) but the speed in which it spread and its ability to self-replicate—in this case over 216,000 endpoints in over 150 countries,[24] 75,000 of those endpoints in 99 countries infected just the first day alone.[25]

Like Shamoon 2.0 and StoneDrill, WannaCry propagated across networks. But WannaCry also successfully spread from network to network. More troubling, perhaps, WannaCry was built on a dangerous vulnerability from the National Security Agency that hacker group Shadow Brokers made available. Now, Shadow Brokers has offered monthly subscriptions of zero-day exploits at $21,000 a month.[26]

The real fear comes from the inevitability that threat actors of all levels will marry tactics that WannaCry used in spreading malware with devastating payloads such as those in destructive malware that delete data and destroy hard drives and that obtaining these types of malware will become increasingly accessible and cheaper than ever before. Given this scenario, how would an organization protect itself from, say, a StoneDrill/WannaCry hybrid?

The experience of a BluVector customer provides some insight. This customer's network is made up of more than 70,000 endpoints. When Shamoon 2.0 hit its network, BluVector's solution sent an alert to the company's IR team, which bricked the affected endpoints and removed the malware from Active Directory in less than seven minutes. Instead of learning about this attack after its system had been affected and risked incomparable damage, the team leveraged BluVector's supervised machine learning technology to discover and destroy the malware in under seven minutes. During that short period of time, BluVector identified the infected machine, provided visibility into any related activity or signs of additional infected machines. All infected machines were bricked and blocked from Active Directory before the Shamoon 2.0 malware had an opportunity to cause any disruption whatsoever.

[23] *Mandiant, 31*

[24] *Schwartz, Mathew J. "Teardown: WannaCry Ransomware." (DataBreachToday, May 17, 2017)*

[25] *Schwartz, Mathew J. "WannaCry Ransomware Outbreak Spreads Worldwide." (DataBreachToday, May 12, 2017)*

[26] *https://steemit.com/shadowbrokers/@theshadowbrokers/theshadowbrokers-monthly-dump-service-june-2017*

BLUVECTOR®

BluVector helps security teams respond to malicious threats up to 80% faster than current approaches. As a leader in Network Security Monitoring & Analytics, BluVector applies supervised machine learning and automation so security teams can detect and respond to advanced security threats at digital speed.

Learn more about BluVector

www.bluvector.io • 571.565.2100