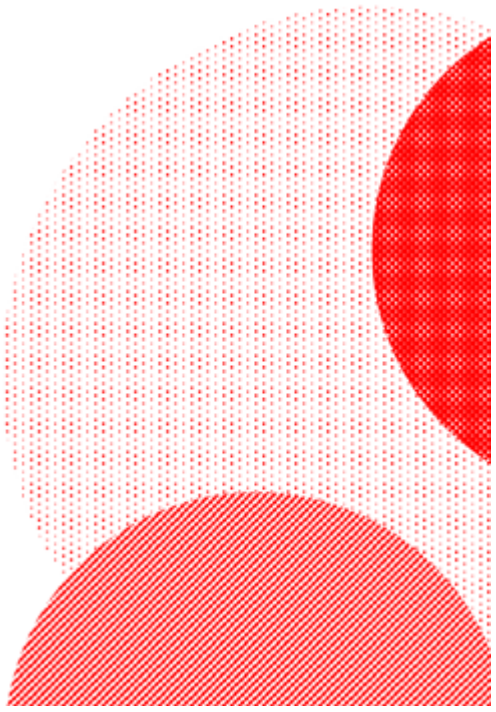
Combating Advanced Malware with Next Gen AV

August 2017

FFRI North America, Inc.



Advanced and Fileless Malware

Advanced malware are persistent malware strains engineered with advanced capabilities for infection, control, data exfiltration and payload execution. The largest threat to client-side attacks is advanced malware.

Fileless malware uses intimate attacks that secretly invade and infect targeted computers, thereby allowing attackers to exploit systems by side-stepping traditional signature based security and forensic tools. Fileless attacks will soon overtake traditional "write-to-disk" attacks which will render legacy antivirus solutions ineffective and useless.

“I consider fileless malware the greatest risk right now,” said Patrick Moorhead, an analyst with Moor Insights & Strategy. “Fileless malware will get a lot worse before it gets better. Since attackers have already had a lot of success and these infections are very difficult to detect, it’s all the rage right now.”

Advanced Malware Threats on the Rise

In 2017, fileless malware has become the largest threat to major worldwide networks. In January and February alone, 140 global enterprises, in every sector, were hit with fileless malware.

“These attacks pose a huge risk because many current antimalware solutions are unable to detect or react to these new forms of attacks,” said Jim McGregor, an analyst with TIRIAS Research. “You have to remember that IT organizations do not upgrade solutions quickly and are often exposed to new forms of attacks; and enterprises are often the early targets because of the potential for valuable information, such as customer data, financial information and emails.”

Companies must recognize the growing threat and protect themselves by reducing and preventing their exposure to all forms of advanced malware attacks. However, many companies are still relying on legacy antivirus software, which has been largely ineffective in detecting advanced malware. Unprepared companies are at risk and vulnerable to costly and damaging intrusions.

Fileless Malware Attacks Raising a Warning

It's been reported that the Russian hack into the Democratic National Committee during the 2016 U.S. presidential race utilized fileless malware and phishing emails, to target specific people or organizations to reveal sensitive information or give unauthorized system access.

Both the U.S. Department of Homeland Security and the New Jersey Cybersecurity and Communications Integration Cell have warned about these kinds of attacks.

(https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf)

(https://www.cyber.nj.gov/threat-analysis/fileless-evasive-intrusion-tactics-pose-challenge-for-network-defense)

"The [NJ Cell] assesses with high confidence that fileless and non-malware -- intrusion tactics pose high risk to organizations, both public and private, and will be increasingly employed by capable threat actors intent on stealing data or establishing persistence on networks to support ongoing espionage objectives or to enable future acts of sabotage," the March, 2017 report noted.

The NJ Cell also reported that most organizations are not currently equipped to defend against fileless attacks.

While these kinds of advanced malware attacks are gaining traction, they're not new to those in the cyber security world.

Yes, fileless malware existed prior to the 21st Century, but it really gained security and media attention in 2001 with Code Red and in 2003 when SQL Slammer was released causing denial-of-service attacks.

Both were fileless malware and both caused a lot of damage and media sensation.

This type of malware resurfaced periodically, but recently it has started to become far more popular with attackers.

"Fileless malware is still relatively new and unfortunately we still are generally unprotected," said Jeff Kagan, an independent technology industry analyst.

"The problem is that now it is quickly beginning to grow and spread. Companies are at risk because these attacks come in phishing emails and are often in a Word document. Once opened, you're infected."

If fileless malware has been around for a while, why is it still so hard to defend against?

Fighting an Invisible Enemy Using FFRI yarai

Fighting an enemy you can't see seems like an impossible task, however, next generation endpoint solutions such as FFRI yarai uses a heuristics component that operates through behavioral analysis on a client-by-client basis. Certain types of advanced malware, such as Ransomware, have a specific set of behavioral characteristics that are common to all infections. FFRI yarai can identify these patterns by using heuristic-based endpoints that stop these forms of behavior based threats, allowing time for the end user to manually authorize the process. FFRI yarai effectively stops the threat before it delivers its full payload.

"The attacks simply are growing in prevalence and scope", according to Pablo Garcia, CEO of FFRI North America, Inc.

“You have to definitely be on your game to detect this stuff,” said Garcia. “There are very few security vendors who can handle these types of advanced attacks because it takes a new approach to malware prevention.”

Traditional anti-virus software has been more reactive than preventative. Legacy AV relies on a database of known characteristics or signatures that have been written on hard drives.

FFRI yarai (http://www.ffri.jp/en/index.htm) is uniquely different because it uses advanced methods, including proactive heuristics and machine learning to analyze behaviors instead of hunting for typical malware signatures.

FFRI yarai automatically prevents attacks before they begin,” said Pablo Garcia. “We use machine learning to catch behavioral changes that signal an attack – even malware attack's that have not yet been identified in the wild. FFRI yarai can determine behavior and characteristics of malicious attacks. The FFRI yarai platform, has prevented over 100 zero-days in the wild, long before public disclosure by third party companies. That’s critical to keeping an enterprise safe.”

"The FFRI yarai agent utilizes five purpose built detection engines to identify, prevent, and quarantine the most advanced cyber threats. Our layered precognitive defense is the key to our success in identifying and stopping advanced threats."

“We don’t rely on signatures because the threats are always morphing and changing,” said Garcia. “Malware names change and attacks change. In today's world malware is a constant concern. With the onslaught of advanced attacks, it’s not a matter of IF it will happen, it's about WHEN it will happen. It’s purely a numbers game, for the bad guys. There are highly crafty people who carry out these attacks and you always have to be on guard."

FFRI yarai Customer Experience

Emerson Stamps is a Network Assistant Manager at DENSO Products and Services America, Inc., located in Long Beach, CA., one of the largest global automotive suppliers of advanced technology, systems and components.

For Stamps, turning to FFRI's security software was a matter of getting ahead of an oncoming problem. It was also a matter of saving their IT workers' valuable time and attention.

"Advanced malware has been a problem for a while, but in the last two or three years it's really become a problem that impacts business," said Stamps, who has worked for the automotive supplier for the past 17 years. "Our standard anti-virus packages just weren't doing enough."

He noted that the company, which had been using traditional anti-virus software, has not been hit by advanced malware, in particular, but that's because he had two network administrators spending three to four hours a day protecting the network.

"We were doing a lot of research, spending our admins' time and efforts trying to stay ahead of what we needed to block," said Stamps. "We were dealing with attachments and emails. It took on a life of its own. The anti-virus packages are just not enough," he added.

Before deploying FFRI yarai, DENSO's network administrators were spending valuable time protecting their system from advanced malware attacks. After deploying FFRI yarai, they have more time to spend on help desk calls and on training and quality checks.

During testing in which DENSO's IT team detonated malware and ransomware on a local area network (LAN), FFRI yarai, stopped all 25 payloads detonated while testing on the new product release.

"This works for us," said Stamps, who noted that they've been using FFRI yarai since October of 2016. "It works well with our anti-virus package. There have been no issues with it bumping heads with other programs. This really reduces the risk of anything happening."

It also has freed up his network admins' time and focus.

"Now we have just one person keeping an eye on what's happening," said Stamps. "It doesn't interrupt our daily operation. We get a report back on any anomalies. It's really, really awesome. It's definitely helped us to lessen the headache and manpower needed to deal with malware attacks."

"We are definitely more secure."

FFRI North America, Inc.
65 Enterprise 3rd Floor
Aliso Viejo, CA 92656
Email: sales@ffri-inc.com