DAMBALLA

Behind Today's Crimeware Installation Lifecycle:
How Advanced Malware Morphs to Remain Stealthy and Persistent

Introduction

The distribution and installation of malicious and unauthorized software has evolved consistently throughout the 21st Century. The evolutionary path from annoying viruses, to destructive malware and on to financially driven crimeware, is well documented and can even be traced through the parallel evolution of technologies designed to counter each aspect of the then contemporary threat.

> **Much of the newest innovation (in malware) has occurred in the methods and mechanisms that install, update and regulate the control of the crimeware installed upon the victims computing device.**

While the individual technologies embedded within crimeware have evolved incrementally – and some people argue today that the rate of innovation has slowed down over recent years – the diversity in which these technologies are applied to fraudulent and criminal ventures has accelerated. Or, to put it another way, professional cyber criminals have been increasingly inventive in ways in which to apply a "standard" toolset of malware features to the way they conduct their criminal ventures.

As traditional malware features continue to consolidate into professionally maintained and purchasable crimeware construction packs with 24x7 support and guaranteed "Fully Undetectable" (FUD) service level agreements, much of the newest innovation has occurred in the methods and mechanisms that install, update and regulate the control of the crimeware installed upon the victims computing device.

Misinterpretation of legacy malware propagation processes and failures in understanding the innovation and dynamism of modern crimeware installation techniques pose a significant risk to businesses facing off against an onslaught of highly motivated cybercriminals. Incorrect assumptions and an outdated understanding of the threat have resulted in organizations pursuing ineffective protection strategies and a bewildered reactive response to successful breaches.

This paper **examines the advancements of legacy malware installation techniques and those currently employed by professional cybercriminals.** By understanding the modern crimeware installation lifecycle and exposing the reasoning behind each criminal tactic, organizations under the crosshairs of their attackers will better appreciate the limitations of the security technologies they currently deploy and will ideally be armed with the intelligence they need to develop more robust protection plans and incident response handling strategies.

How the Malware Lifecycle Worked in the Past

In years gone by, the infection-installation lifecycle of viruses was relatively simple to understand. A computer would become infected via an infection vector (such as tainted removable media), a solitary virus binary would be placed within the computer, registry and start-up settings would be modified, the virus would launch and badness would happen. Eventually a copy of the virus would fall into the hands of the anti-virus vendors, detection signatures would be crafted, cleanup scripts would be created, and anti-virus products would be updated. The net result was a reassuring, but endless, game of whack-a-mole.

For a long time, the simplified one-step, two-step dance that was the virus lifecycle served its purpose. Organizations gained an appreciation of the threat and confidence grew in the anti-virus' ability to counter (and mitigate) the threat.

As virus authors continued to hone their capabilities and unveiled new ways in which to monetize their malicious software, additional steps were incorporated into the installation lifecycle to facilitate more robust and scalable criminal endeavors. **A critical step added to the lifecycle was the development and incorporation of "dropper" and "downloader" strategies.**

The terms "dropper" and "downloader" are often used interchangeably today as the differences between the two classes of malware have become indistinguishable as time goes by.

1) Droppers were originally distributable software packages that contained multiple malware components. A dropper would automatically install its payload of malicious agents, disable the victims' security and monitoring software, seek to hide core components and obfuscate its activities. Once completing these tasks it would start up the core malware agent.

2) Downloaders were designed to perform the same actions as Droppers – disabling the victims' security and monitoring software, hiding core components and obfuscating the infection vector, etc. – but tended to be smaller than Droppers because they did not contain the core malicious library components. Instead of unpacking an embedded copy of the core malware agent, the Download would connect to a remote file repository and download the core component(s).

The purpose of incorporating droppers and downloaders into the installation lifecycle was two-fold for the cyber criminals – it offered new potential for evasion, and facilitated a federated solution ecosystem.

How the Idealized Dropper Lifecycle Works

1) The self-contained **dropper binary** is downloaded by the computer after falling victim to an exploit or succumbing to social engineering.

2) The dropper is executed and proceeds to unpack and install components – executing embedded commands.

3) Components of the dropper attempt to disable security settings, modify configuration settings and ensure that the main malware components will be executed automatically after system restarts.

4) Evidence of the infection vector and system modifications is deleted or obfuscated.

5) The original dropper package, along with nonessential components that were extracted from the dropper, are deleted from the victim's computer and the core malware component is ready for use.

6) The core malware component contacts the criminals CnC infrastructure and waits for new commands.
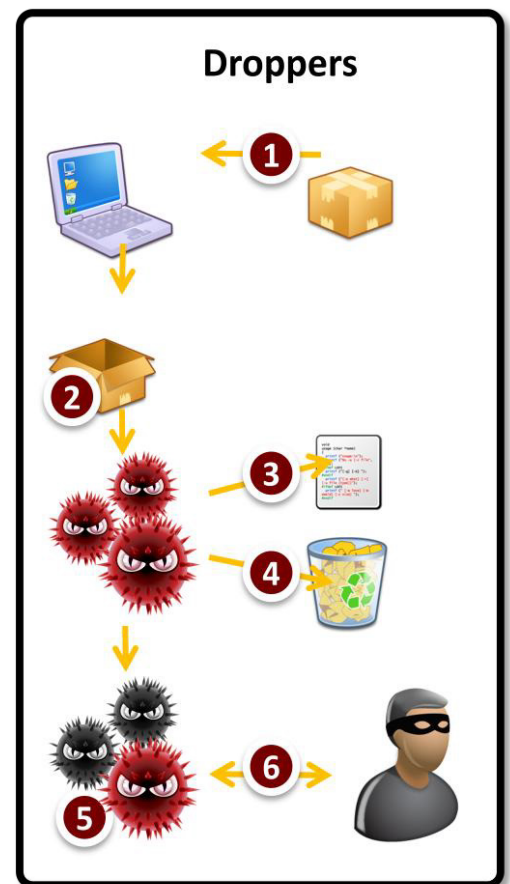
How the Idealized Downloader Lifecycle Works

1) The **downloader binary** is downloaded by the computer after falling victim to an exploit or succumbing to social engineering.

2) The downloader is executed and proceeds to unpack and install temporary components – executing embedded commands.

3) Components of the downloader attempt to disable security settings, modify configuration settings and ensure that the main malware components will be executed automatically after system restarts.

4) Downloader agents connect to a remote file repository and download the core malware component.

5) Evidence of the infection vector, the downloading of the core malware component and system modifications are deleted or obfuscated.

6) The original downloader package, along with nonessential components that were extracted from the downloader, are deleted from the victim's computer and the core malware component is ready for use.

7) The core malware component contacts the criminals CnC infrastructure and waits for new commands.

How the Idealized Downloader Lifecycle Works

Today's threat has become incredibly complex due to an increasingly federated crimeware support and monetization model. The breadth and depth of malicious technologies and cybercrime services that are on offer – for sale, rent or hire – is staggering, and the list continues to grow daily.

This complex relationship between cybercrime tool producers, content distribution services, hosting facilities, resilient CnC topology and the actual criminals orchestrating an attack is most apparent in the crimeware installation lifecycle. While malware is insidious, as a point of differentiation Crimeware can be considered the grownup siblings of everyday malware. Crimeware is carefully selected for the monetization of the victim and the profiteering of the criminals managing the infectious campaign.

For many victims attempting to come to grips with a successful crimeware breach within their organization, a failure to understand and appreciate the inner mechanics of the crimeware installation lifecycle often causes them to misinterpret forensic data. This failure causes their organizations to arrive at incorrect conclusions about their adversary and to subsequently launch ineffective and incomplete mitigation processes.

While droppers or downloaders are core components of a cybercriminals arsenal, they tend to be used inmore sophisticated and voluminous ways than most victims realize. A monetization opportunity at each stage of the crimeware installation lifecycle has resulted in multiple "attacks" being launched and managed simultaneously.
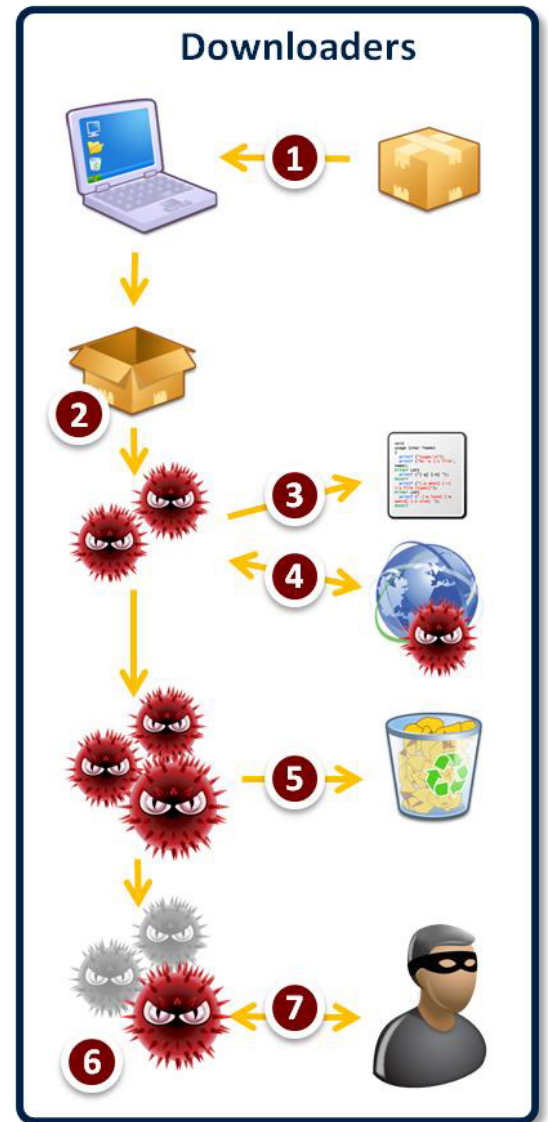
For example, "pay-per-install" business models have resulted in the development of affiliate systems for the installation of third-party droppers. In such business models, participating cybercriminals can increase their rewards by installing multiple droppers on a single victim.

As such, there is a growing trend for compromised computers to be infected with multiple crimeware packages (under the CnC management of multiple distinct cybercriminals) simultaneously.

### How the Crimeware Installation Lifecycle Works

Modern crimeware installation involves more steps than the idealized (and largely outdated) dropper or downloader lifecycles. Today's installation lifecycle incorporates many checks, balances and resilience features – as a means of maximizing the success of the installation, and protecting the participating cybercriminals.

1) A self-contained dropper binary is downloaded by the computer after falling victim to an exploit or succumbing to social engineering. In many cases **multiple droppers** will be forced on to the victim's computer as part of a pay-per-install scheme.

2) The dropper is executed and proceeds to unpack and install components – executing embedded commands. If multiple droppers were placed upon the victim's computer, then they too will be executed in parallel.

3) Components of the dropper attempt to disable security settings, modify configuration settings and ensure that the main malware components will be executed automatically after system restarts.

A component of the dropper package proceeds to confirm the installation success with an external crimeware update site. The update site ascertains whether the "victim" is real and whether it has been seen/compromised before.

4) The update site will return updated configuration and download location information to the installed dropper component – providing fresh instructions on how to acquire the core crimeware agent.

5) A component of the dropper package uses the fresh configuration information to locate the crimeware download site – and then proceeds to download the main crimeware toolpack.

In some cases this may be a separate downloader package, or may be multiple crimeware packages (representing a variety of cybercrime organizations and botnets).

6) The downloader package is executed and proceeds to unpack, install and replace key crimeware components. If multiple downloaders were retrieved, then they too will be executed in parallel.

Crimeware Installation
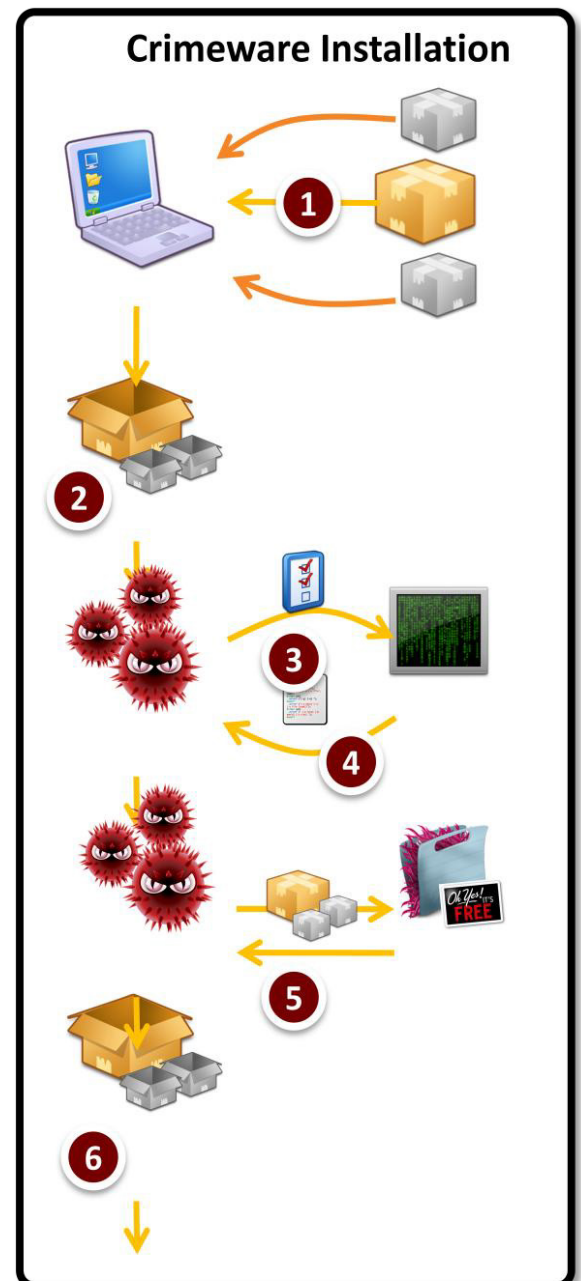
7) The original dropper package, along with non-essential components that were extracted from previous dropper and downloader phases, are deleted from the victim's computer and the core crimeware agent is ready to begin operation.

The crimeware agent performs a number of built-in functions – such as scraping software license keys, password files and authentication credentials stored or cached by the victim's Web browser – and automatically proceeds to upload an encrypted file containing the stolen data to a remote file server.

8) These automatic functions are executed within seconds of installation and are designed for enumeration of the victim's machine and quick monetization. Should the cybercriminal lose access (and control) of the victim, they will still have this valuable information.

The crimeware agent begins to search for, locate and communicate with the frontline CnC servers. The crimeware will typically have a list of possible CnC server locations or may utilize a time-based Dynamic Generation Algorithm (DGA) to locate candidate CnC servers. If a CnC server is unavailable, the crimeware agent will attempt to communicate with the next CnC server in the list until it locates one that is "alive".

8) These automatic functions are executed within seconds of installation and are designed for enumeration of the victim's machine and quick monetization. Should the cybercriminal lose access (and control) of the victim, they will still have this valuable information.

9) The cybercriminal may have some of their frontline CnC servers operating in load-balancing or hotswap modes for resilience.

10) The frontline CnC servers often operate as proxies for communication between the crimeware agen running on the victim's computer and a smaller network of core CnC servers with which the cybercriminal regularly connects. These core CnC servers are responsible for managing and organizing the entire botnet.

11) The cybercriminal regularly updates the crimeware agent installed on the victim's computer. In many cases the cybercriminal will also deploy the pay-perinstall crimeware packages of other botnet operators as a way of "leasing" or "selling" parts of their existing botnet.

12) The cybercriminal regularly updates the configuration files to the crimeware agents (e.g. lists of new frontline CnC servers) and may elect to send commands to the victim's computer interactively or through a batch queuing system.
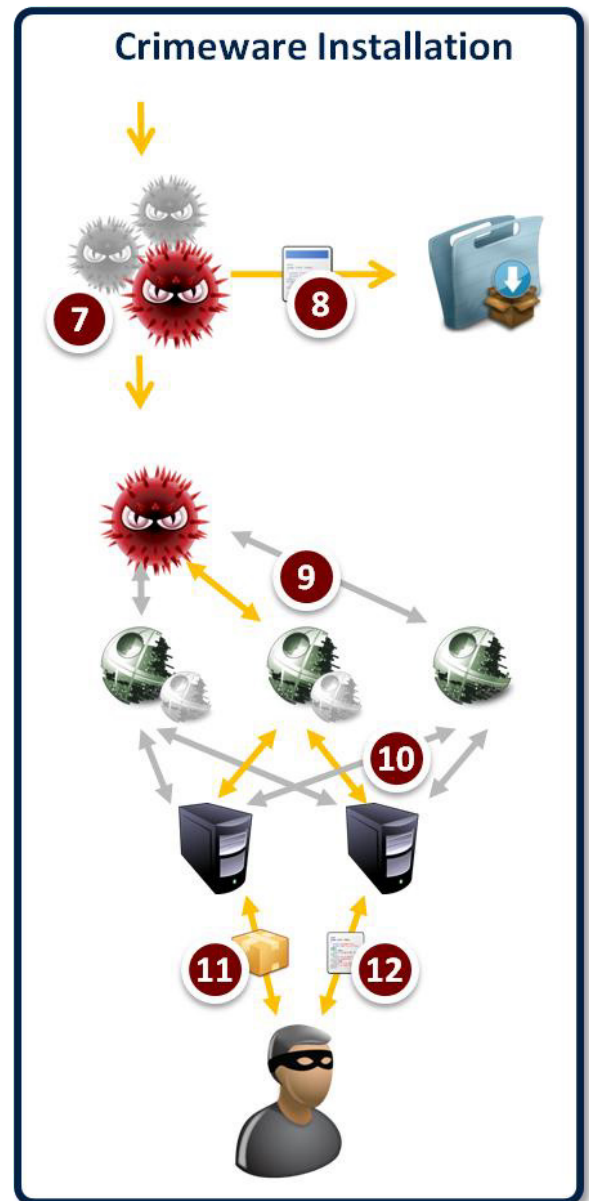
What Today's Crimeware Installation Means for Detection and Mitigation

The modern crimeware installation lifecycle has evolved the way it has for a number of reasons – ranging from the dynamics of the federated cybercrime ecosystem, through to efficiencies in distribution and management – but the most important reasons behind the complexity and sophistication of modern crimeware installation can be attributed to the need to evade detection and survive commonly encountered mitigation techniques.

Each step within a crimeware installation exists for a reason and has numerous consequences for detection and mitigation strategies.

Detection Consequences

The approach cybercriminals have adopted for the distribution and installation of their crimeware evolved out of necessity in order to bypass the detection technologies deployed by their prospective victims. Key components of the crimeware infection lifecycle designed to evade detection include the following:

› Dropper and downloader components are typically "armored". Using a variety of packers, crypters and inspection-detection engines, crimeware authors can ensure that common debugger and emulation analysis techniques will not work. The addition of a**dvanced anti-virtual machine analysis technologies is commonly a click-box** in a crimeware armoring toolset.

› Many crimeware packages include toolsets for automatically disabling host-based detection technologies – **disabling anti-virus** and IDS products installed on the victim's computer, changing local DNS settings to ensure that no future updates to the operating system or packages are possible, and adding tools that recheck (and re-disable) protection settings frequently.

› Droppers and downloaders can be created in real-time by the cybercriminal or created in advance at rates in excess of 10,000 per hour. By effectively **creating a "unique" malware component** each time, static-analysis and hash-based detection technologies are bypassed.

› The use of droppers and downloaders at the initial stage of the infection lifecycle means that the core crimeware agents aren't exposed directly – i.e. broad-spectrum attack vectors may be used to initially exploit vulnerable computers which will be detected promptly by security vendors, but the actual crimeware agents will only be installed on successfully compromised and verified vulnerable computers.

› The initial malware packages include cleanup components **designed to remove all evidence** of the initial compromise vector.

› The downloader strategy has an advantage over the dropper strategy when it comes to detection. By not distributing core crimeware components within the initial package, the attacker can be more selective with what they distribute – ensuring more timely and evasive components, and controlling their selective distribution (which is important to the third-parties that operate within this phase of the cybercrime ecosystem).

› By performing a quick inventory of the victim's machine at the dropper/downloader stage and submitting that to the crimeware distribution site, the c**ybercriminals can verify that the compromised computer is real** (and not some analysis system) and respond accordingly. In some cases, upon discovering that the "victim" was faked or is an automated analysis system, the cybercriminals launch DDoS attacks against the corporations IP addresses or initiate more targeted and personalized attack campaigns.

❯ Most malware does not encrypt outbound network communication. Critical data stolen from the victim's computer is typically packed and file-encrypted at the host-level before sending over a "clear text" network protocol such as HTTP and SMTP – thereby **evading anomaly detection systems and data-leakage prevention systems** (DLP).

❯ The criminal operators of the botnet will push down new bot agents frequently (after verifying that they already evade the anti-virus suites installed on the victim's computer) – often updating core components daily.

Mitigation Consequences

Beyond detection of the crimeware, there are a number of mitigation consequences:

> **Some cybercriminals elect to leave some trace evidence behind along with nonessential and disposable malware components.**

❯ Modern malware is designed to receive updated configuration files frequently. While the initial packages will "ship" with default configuration data – often including a list of a dozen-plus possible sites to download core crimeware components – they will also seek new settings information to overcome the loss, takedown or blocking of core distribution and CnC services.

❯ While many droppers and downloader packages include cleanup components that remove evidence of their installation (and compromise vector), some cybercriminals elect to leave some trace evidence behind along with nonessential and disposable malware components.

When the malware is discovered by the victim they may attempt to clean up the compromised computer and not discover the other hidden cybercrime components.

❯ The inclusion of third-party crimeware distributors at the post-dropper stage means that multiple crimeware packages may be installed mid-cycle of the infection lifecycle – making it impossible to "clean up" the victim's computer. Increasingly these crimeware packages will be under the control of different criminal organizations – resulting in multiple criminal entities having interactive access to the compromised computer.

❯ Many malware contain default built-in functions designed to inventory the system and retrieve commonly stored personal and confidential information. Data such as license keys, VPN and encryption certificates, stored and "remembered" passwords, locally-stored documents with key words such as "password", "confidential" and "secret", are automatically packed into a datafile, encrypted, and sent to a remote file server.

This process may only take a few seconds after the initial successful installation of the crimeware package – and is designed to provide a cache of retrievable data to the attacker should their infiltration be detected, and provides off-line storage of information independent of their CnC infrastructure. Since the data is encrypted, the data may be uploaded to free and public file-hosting services – without fear of law enforcement or competitor involvement.

❯ The core crimeware agent will receive updated configuration file data frequently. This data will include lists of new CnC infrastructure – reflecting any changes due to law enforcement takedown and newly created CnC systems.

❯ To overcome CnC takedowns, cybercriminals make use of multi-tier CnC infrastructure designs. The frontline CnC servers are generally considered disposable and may have a number of "hot-standby" servers ready and waiting in case of a server outage (due to takedown, etc.). These frontline servers proxy commands and data to the core CnC servers – with which the cybercriminal liaises anonymously.

Conclusion

Today, cybercriminals have the upper-hand – and will likely retain it in to the future despite advances in malware detection strategies and CnC takedowns. The cybercrime infection lifecycle has evolved to encompass a number of "commercial" managed service provisioning models that allow for third-parties to contribute and augment the cybercrime and the subsequent fraud.

As the security industry strives to counter the threat in whack-a-mole fashion, the cybercriminals will continue to innovate and streamline their operation. In the near future, the crimeware lifecycle will continue to evolve in the following ways:

> **Malware droppers and downloaders will remain the "mule" of crimeware** and will continue to become more "personalized" to the prospective victim. More advanced interactions with the criminal's distribution services will ensure that one-time single-use URI's and malware will become the norm – protecting the criminal organization from automated detection and enumeration by security vendors.

> The pay-per-install model for malware content provisioning will cause a **growth in the number of crimeware installed per victim computer.** Today, the majority of computers are infected with just one crimeware agent at a time. This has been changing and will inevitably cause the majority of computers to receive multiple crimeware installations with each compromise.

> The CnC infrastructure will become more resilient to takedown processes. While security vendors and law enforcement agencies are becoming more proficient in taking down the criminals frontline CnC servers, the cybercriminals are becoming more proficient in bringing up resilient servers and segregating their botnets to ensure that not all data or computers are lost. Botnet CnC infrastructure will increasingly make use of third-party botnets for hosting as more cybercriminals build out their third-party support platforms.

> Already the use of **Domain Generation Algorithm (DGA) technology within the core crimeware agents has been used effectively to bypass domain blocking technologies and blacklists,** and the technique will become more accessible as popular crimeware DIY kits incorporate the feature.

> The **frequency of crimeware updates to the victim computers will continue to rise** in the face of cloud-based anti-virus solution provisioning. Already several crimeware families utilize "machine locking" features (similar to commercial license verification and enforcement capabilities) to ensure that the crimeware component will not function on any system other than the intended victim – thwarting any cloud-based analysis technology.

> As the security industry strives to counter the threat in whack-amole fashion, the cybercriminals will continue to innovate and streamline their operation.

Further Reading

"Extracting CnC from Malware", Damballa, 2009
"Serial Variant Evasion Tactics", Damballa, 2009
"Botnet Communications Topology", Damballa, 2009
"Advanced Persistent Threats (APTs)", Damballa, 2010

About Damballa

As the experts in advanced threat protection and containment, Damballa discovers active threats that bypass all security prevention layers. Damballa identifies evidence of malicious network traffic in real time, rapidly pinpointing the compromised devices that represent the highest risk to a business. Our patented solutions leverage Big Data from the industry's broadest data set of consumer and enterprise network traffic, combined with machine learning, to automatically discover and terminate criminal activity, stopping data theft, minimizing business disruption, and reducing the time to response and remediation. Damballa protects any device or OS including PCs, Macs, Unix, iOS, Android, and embedded systems. Damballa protects more than 440 million endpoints globally at enterprises in every major market and for the world's largest ISP and telecommunications providers.

To learn more about Damballa Failsafe visit our website www.damballa.com, contact us at 404.961.7400 or follow us on Twitter @DamballaInc.