Related Insights

info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak

December 20, 2014

Get The Latest Insights

By The PhishLabs Team | December 19, 2014

In a recent blog post, we wrote about Vawtrak expanding targets and gaining momentum. Fast forward a few months and the threat is anything but diminishing. Sophos just released a technical report on Vawtrak which discusses the significance of the threat and its Crimeware-as-a-Service model. In December 2014, Vawtrak version 0x38 was released including significant code and configuration changes that indicate momentum and an intense focus on development of the crimeware kit. To better understand the complexity of the threat, this post is a historical review bringing you all the way up to the most recent enhancements observed in December.

First, a few key points about Vawtrak and its capabilities:

- Sophisticated, modern banking Trojan
- Small, efficient client written in MS Visual C
- Sophisticated botnet management back-end
- Polymorphic
- All standard spyware functions (keylogging, etc.)
- Advanced Man in the Middle webinjects capabilities
- Downloadable configuration
- Development controlled by capable and experienced cybercriminals

Roots in, you guessed it…Russia

In the early to mid-2000's, Nikita Kuzmin, a 25-year-old Russian national (the admitted inventor of Gozi) worked on coding spyware and Remote Access Trojans (RATs). He borrowed source code from existing families popular at the time, proxy functionality common in a couple of kits, spyware functionality from the codebase of UrSnif (developed by Alexey Ivanov, "subbsta"), and botnet C2/management functions and backend code from Nuclear Grabber (based on A311 Death/Haxdoor maintained by Corpse).

Kuzmin worked closely with the VXer (computer Virus eXperts) superstars of those days: Corpse, Vladislav Horohorin (BadB), the Vasiliy Gorshkov and Alexey Ivanov team (Suidroot, Eliga, XTZ, Skylack, Kotenok). He had known some of them since the ShadowCrew days. He was younger than most of his peers, at the time posting that he was looking forward to

getting his “А водительские права” (Russian motorcycle/class A driver license) and hoping to soon be making enough money for a brand-new, “real” motorcycle, so he could finally retire the decrepit Мопед Карпаты scooter he picked up on the scene after someone had crashed or ditched it. Despite his young age, he was trusted, respected for his practical technical skills and coding talent, and also known for his enthusiasm for the idea that Internet fraud, especially against Western targets, was a legitimate profession with better pay and perks than working for local computer and software retail outlets, university labs, and ISPs.

Cybercrime-as-a-Service emerges

Through his VXer contacts, Kuzmin had access to the source code for several crimeware kits with overlapping state-of-the-art capabilities, each kit doing something exceptionally clever in one key area compared to the others. With the help of a close affiliate of the HangUP Team, they created a repository under version control for a crimeware kit codebase incorporating all of these best features – this is what became known as Gozi. The HangUP team was a nationalistic group with a common following of “cyberfacism,” shared Russian and Nazi imagery, and an overarching theme to wage financial warfare on Western interests through the use of the Internet to commit fraud.

Kuzmin and his partners launched their first major operation, 76service, in a beta phase in 2006 and opened it up as “cybercrime-as-a-service” (CaaS) or “criminal-to-criminal” (“C2C”) services operation to customers from the Internet fraud underground scene in early 2007. Kuzmin’s partners, in the then brilliantly innovative Gozi/76Service, were Aleksandr Kalinin, also known as Grig (who also used the handles “tempo” and, for the purposes of marketing the service, “76”) and the systems administrator, a Latino man (known as Exoric) in North America who spoke Spanish and maintained the relationship with their incubator project’s bulletproof hoster in Panama. To this day, Kalinin is still at large in Russia and is implicated as part of the ring involved in breaches at TJX, Heartland, and NASDAQ.

Gozi Exposed

The first samples from Kuzmin’s production-ready Gozi kit were collected and analyzed in 2007, subsequently exposing 76service and bringing to an end the period in which the operation could thrive without disruption by cybercrime fighters.

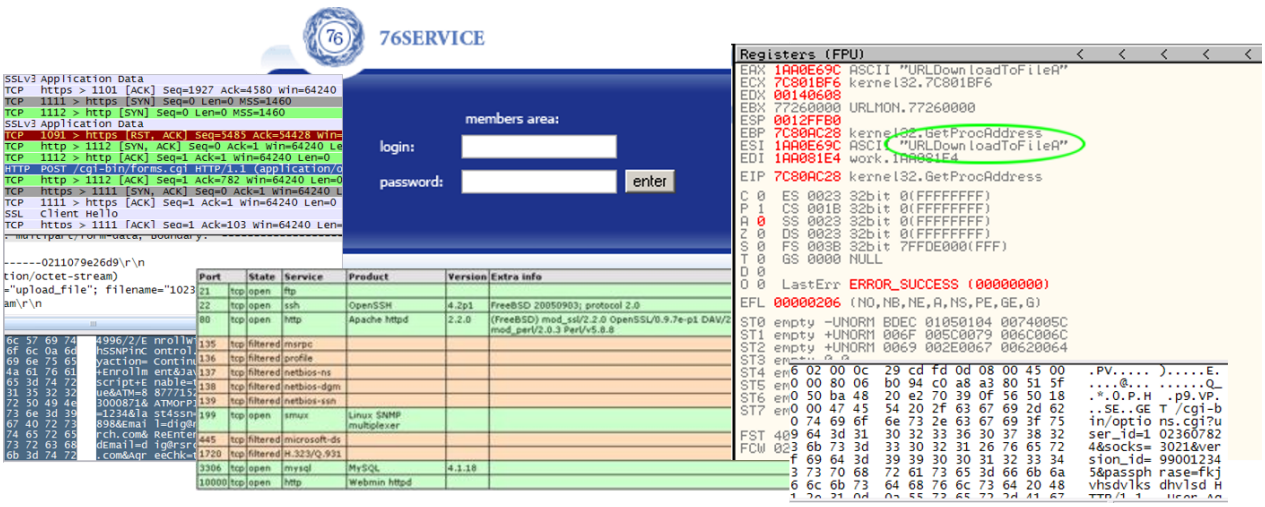


Figure 1. Analysis of early Gozi code in 2007. [Source: Dell SecureWorks]

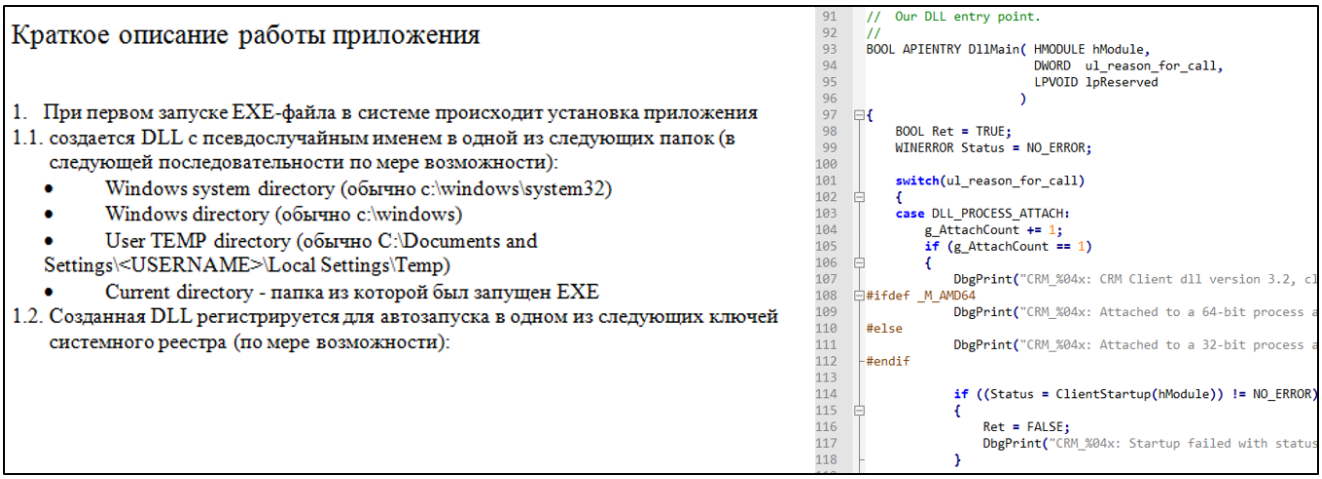
Competition heats up – Gozi 2.0

Looking to compete with kits like Zeus, Kuzmin worked with other partners from the HangUP Team between 2007 and 2009 to refactor a lot of the code and incorporate some of the latest tactics from more current codebases. To fund this, thinking the new version in the works would make Gozi 1.0 obsolete, Kuzmin sold the source code for a reported $50,000 plus a profit-sharing arrangement. His buyer was another hacker and old contact, a seasoned cyberfraudster using the handles NSD and 01NSD (from a transliterated abbreviation of “несанкционированный доступ”, translated as “unauthorized access”) with a reputation going back at least to HangUP Team days in 2005.

Frustrated with new development efforts, Kuzmin hired Deniss Čalovskis (from Latvia, using the handle “Miami”) in September 2010 to replace Corpse’s formgrabber code with full-featured webinjects capability that could not only read but write/modify (man-in-the-middle) web sessions like Zeus and Torpig/Anserin/Mebroot. This was to become the Gozi 2.0 version.

Gozi 1.0 source code leaked

On September 20, 2010, Kuzmin sent Čalovskis a RAR file of the “Gozi 1.0″ source code so Čalovskis could work on webinjects. The Gozi kit’s actual name is “CRM” and the RAR file included CRM version “5557” with a build date of 2010-09-16. It was the latest known version, capable of using a pre-computed list of domain names for C2, which used a combination words from the US Constitution based on the bot group ID and a date in the format MM/YYYY. Negligent to password protect the file, the code was discovered and leaked; anyone interested could download the unencrypted, password-less source code, too.



Краткое описание работы приложения

1. При первом запуске EXE-файла в системе происходит установка приложения
1.1. создается DLL с псевдослучайным именем в одной из следующих папок (в следующей последовательности по мере возможности):
   - Windows system directory (обычно c:\windows\system32)
   - Windows directory (обычно c:\windows)
   - User TEMP directory (обычно C:\Documents and Settings\<USERNAME>\Local Settings\Temp)
   - Current directory - папка из которой был запущен EXE

1.2. Созданная DLL регистрируется для автозапуска в одном из следующих ключей системного реестра (по мере возможности):

```
91  //  Our DLL entry point.
92  //
93  BOOL APIENTRY DllMain( HMODULE hModule,
94                         DWORD  ul_reason_for_call,
95                         LPVOID lpReserved
96                       )
97  {
98      BOOL Ret = TRUE;
99      WINERROR Status = NO_ERROR;
100
101     switch(ul_reason_for_call)
102     {
103     case DLL_PROCESS_ATTACH:
104         g_AttachCount += 1;
105         if (g_AttachCount == 1)
106         {
107             DbgPrint("CRM_%04x: CRM Client dll version 3.2, cl
108 #ifdef _M_AMD64
109             DbgPrint("CRM_%04x: Attached to a 64-bit process a
110 #else
111             DbgPrint("CRM_%04x: Attached to a 32-bit process a
112 #endif
113
114             if ((Status = ClientStartup(hModule)) != NO_ERROR)
115             {
116                 Ret = FALSE;
117                 DbgPrint("CRM_%04x: Startup failed with status
118             }
```

Figure 2. Gozi v1.0 source code leak.

Gozi 2.0 goes live

Beginning in late 2010, Kuzmin worked with “Daniel” Mihai Ionut Paunescu (using the handle “Virus”) at PowerHost in Bucharest, Romania, to setup and host multiple botnets using this webinjects-capable Gozi 2.0 against banks in Europe, the UK and the US.

Kuzmin detained and charged

After webinjects were incorporated and “Gozi 2.0” went gold/GA, Kuzmin was arrested in California, pleading guilty six months later and leaving NSD with v1.0 and Čalovskis with v2.0 to carry on ad hoc cybercrime operations using Gozi botnets.

Public attacks against U.S. banks

Pictured: vorVzakone and another partner in the flagrant video promoting their “freemium” services

In 2012, someone, most likely Čalovskis, made the new code available to Oleg Vsevolodovich Tolstykh (a.k.a. “Sergey”, “Serega”, and “vor v zakone” translated as “thief-in-law”, and the related handles “vorVzakone” and “vorVzakon”) and Kuzmin’s old friend, NSD. The three launched a very public campaign known as Project Blitzkrieg – a series of attacks on U.S. banks specifically, using rejuvenated Gozi 2.0 code with a new backconnect SOCKS proxy feature. This version was designed not just to run on 64-bit systems, but it was the first known crimeware kit to actually use webinjects in a 64-bit browser.

Gozi operations in full swing after arrests

With Kuzmin detained in the U.S., reportedly cooperating with authorities, and vorVzakone running the show in Russia as NSD took over the code, it made almost no impact on day-to-day Vawtrak/Gozi 2.0 operations when Kuzmin’s former compatriots in crime were finally arrested in November (Čalovskis arrested in Latvia) and December (Paunescu arrested in an FBI-directed raid of PowerHost in Romania) of 2012.

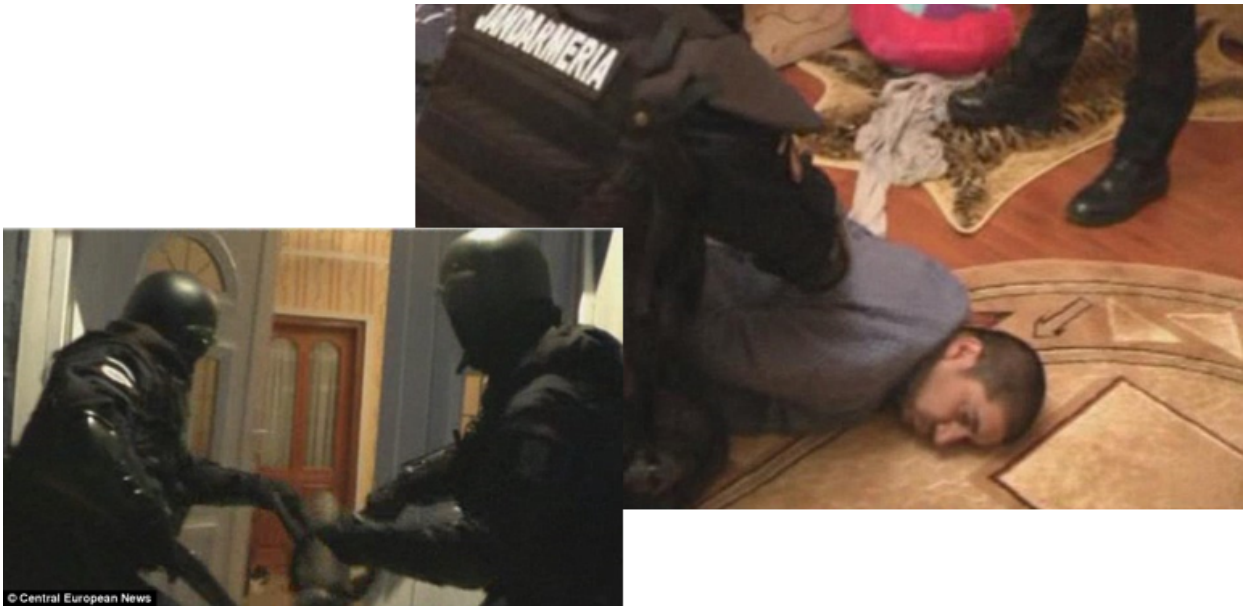


Figure 3. PowerHost raided and Mihai Paunescu arrested in Romania, December 2012 [Images source: Central European News]

With a little help and possibly inspiration from the power vacuum created by these arrests, this capable vorVzakone+NSD partnership aspired to be the founder of a cyberfraud syndicate. They provided a builder kit with a manual (but not the source code) and boot-camp style training for wannabe botmasters in exchange for “educational fees” and a share of profits in what vorVzakone described as a “freemium” software business model. Being a consummate marketer, vorVzakone dropped the old “CRM” name and adopted the Gozi name by which it was known worldwide, calling it “Gozi Prinimalka” (the latter word from the Russian meaning “to receive”).

In vorVzakone's playbook, his crew would setup and use a bank of cheap computer running Skype to flood the account the holder's phone line while their account is being raided, to prevent them from receiving confirmation calls or SMS alerts from their banks.

By Spring 2013, vorVkazone and NSD had found some partners whose capabilities and allegiances were vetted through participation in their program. Collectively, they became known as the Neverquest crew.

Neverquest Crew

Neverquest operations have ditched blocking victims phone lines with Skype, since voice and SMS OoBV is used more often than ever to verify the types of transactions used to raid accounts. They have since begun using iBanking spyware for Android to intercept both phone calls and SMS, injecting QR codes into pop-ups on the banking site that link to this tool used by Neverquest to subvert OoBV.

Confused by the code's genetics and the association with the payload, the malware family is still referred to variously by the AV industry as "Ursniff"/"Snifula," "Rovenix," "Vawtrak," "Reveton" (ransomware payload), "Neverquest," "Tepfer," and "Dapato," sometimes different names from the same AV engine for the same exact variant downloaded from a different domain name (same packer, same IP address). Gozi 2.0 and later versions were most commonly referred to as "Vawtrak" but the core Trojans are basically the same thing and are all examples of 64-bit Gozi 2.0 "Prinimalka".

The main body of the (Russian) Neverquest Vawtrak crew is still overseen by vorVzakone. They have a client-provider relationship but the Neverquest operations are directed at a high level by him and his partners. In 2014, as part of a post-Project Blitzkrieg operations revitalization effort, that crew added a "bizdev" (business development) section to the targeting configuration in order to steal data that can be mined by back-end processes to identify potential new targets and compromise accounts on other services that might be useful monetizing their efforts.

Targets

One of the early non-financial targets to come out the bizdev concept is StubHub, the eBay-owned event tickets marketplace. Losses to fraud against StubHub totaled USD $1.6 million. Vawtrak was the tool used to compromise the 1600 accounts used to commit that fraud. U.S. and foreign law enforcement launched a coordinated response which resulted in the arrests of seven people across the globe, most of whom had direct business ties with the Russian Vawtrak crew.

Since June 2014, we've seen some slightly out of date, but still full-featured, Vawtrak versions attacking a very small number of banks in Japan on a fairly small scale, perhaps in what are precisely targeted attacks. This is believed to be an Asian crew that graduated from

Project Blitzkrieg. However, with new webinjects and code changes commissioned by a relatively new client of Vawtrak's Russian masters, attacks on Australian banks have grown, and banks in New Zealand have been added to the targeting configuration.

The largest increase is by far the number of North American targets, especially large U.S. financial institutions. It is clear that Vawtrak is a threat quickly growing in size, scale, and sophistication and it is now back on the radar of security researchers, analysts, investigators, and law enforcement after being largely discounted and dismissed for nearly a couple of years.

New version of Vawtrak observed

In December 2014, Vawtrak version 0x38 was released. There were many significant code and configuration changes that indicate momentum and an intense focus on development of the crimeware kit and the service business built on top of the infrastructure provided by Vawtrak botnets. Other observed changes include:

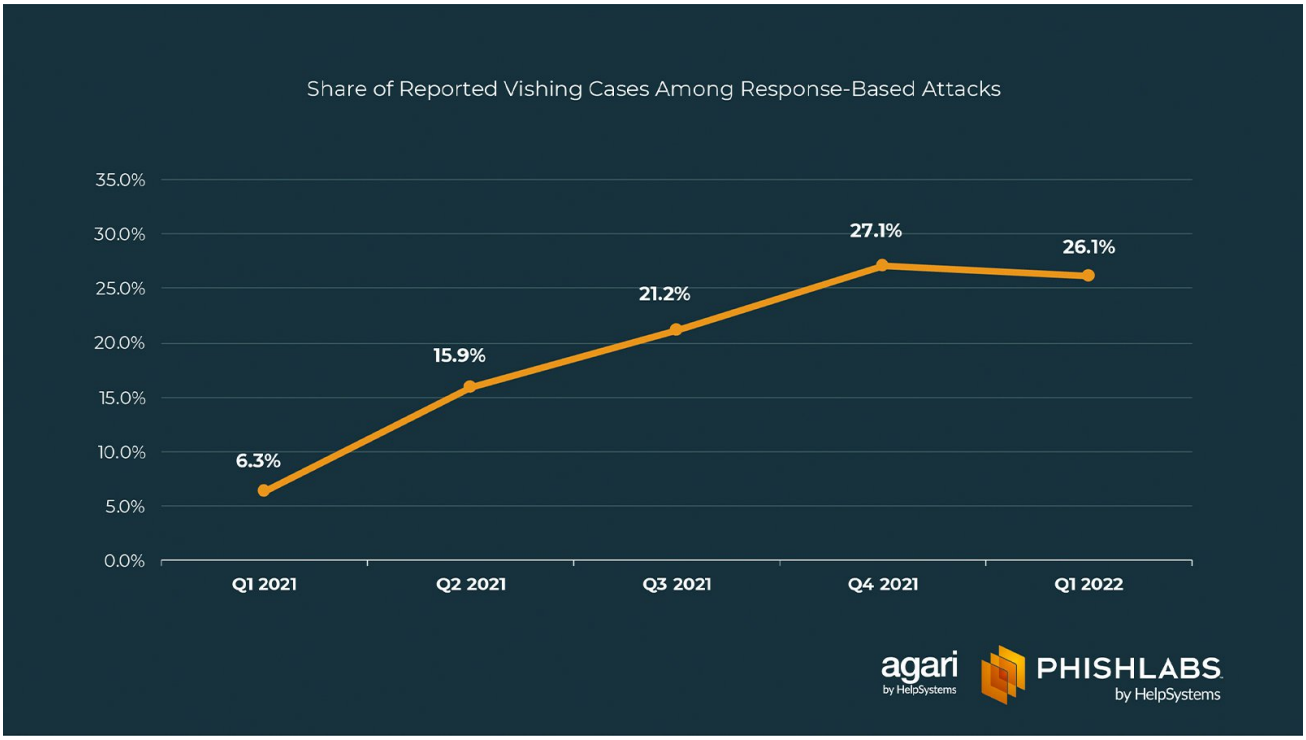
- Significant changes to how the configuration data (with sensitive communications and targeting information) is protected.
- Many more targets and enhanced webinjects.
- Communications template and syntax has changed significantly.
- The bot collects and reports new and more data about the infected system, such as the NetBIOS workgroup or domain name.

We've also seen them respond to the attention they are getting from malware analysts and investigators by finally resorting to the adoption of modern anti-analysis tactics such as virtual machine detection and anti-debugging methods designed to defeat, or at least hinder, forensics and both static and dynamic/behavioral analysis.

That brings us up to the present. Unfortunately, the Vawtrak story is not finished yet, given the following:

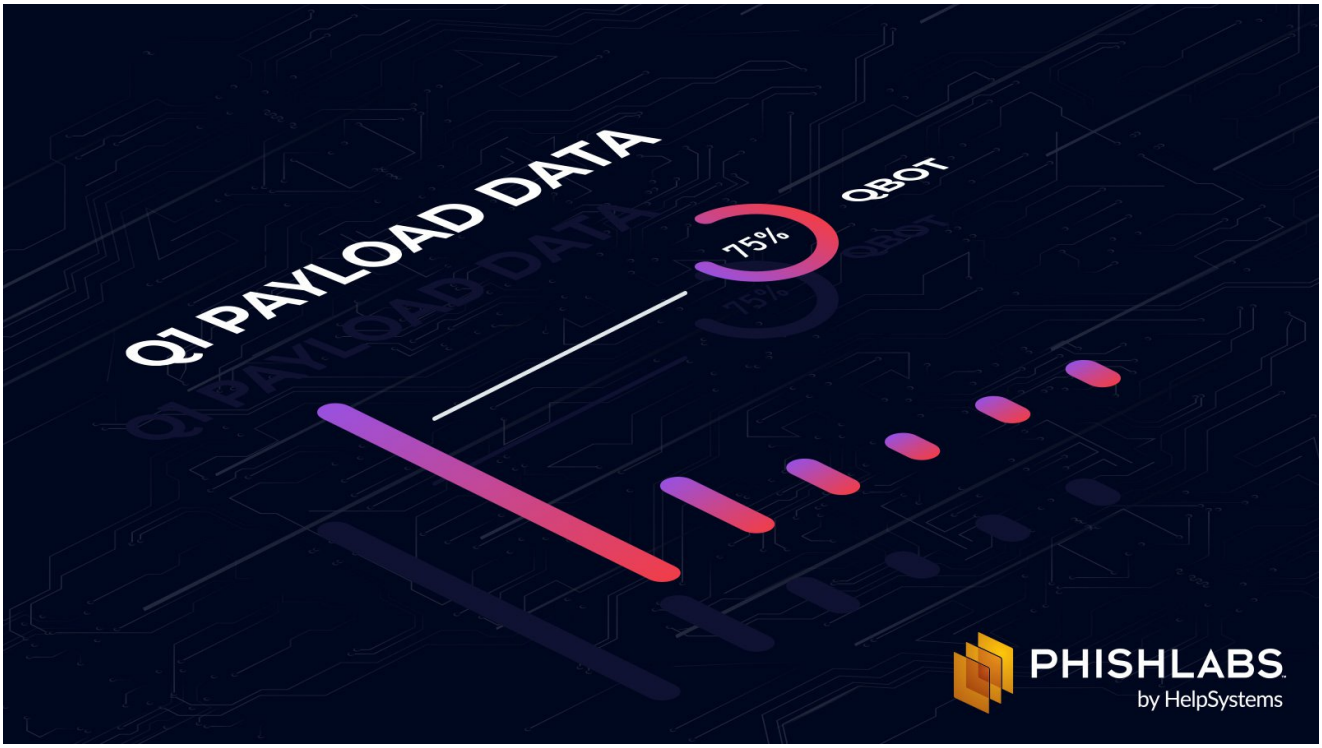
- High scoring results of recent threat modeling exercises applied to Vawtrak and other top threats.
- The trend of significant increase in the activity associated with spambots, exploit kits, and loaders directly tied to Vawtrak distribution.
- Significant changes in the very latest iterations/versions of the malware.

It is predicted that we are headed toward a new and dangerous chapter in the Vawtrak story. Follow our blog as we continue to closely track this threat and others.



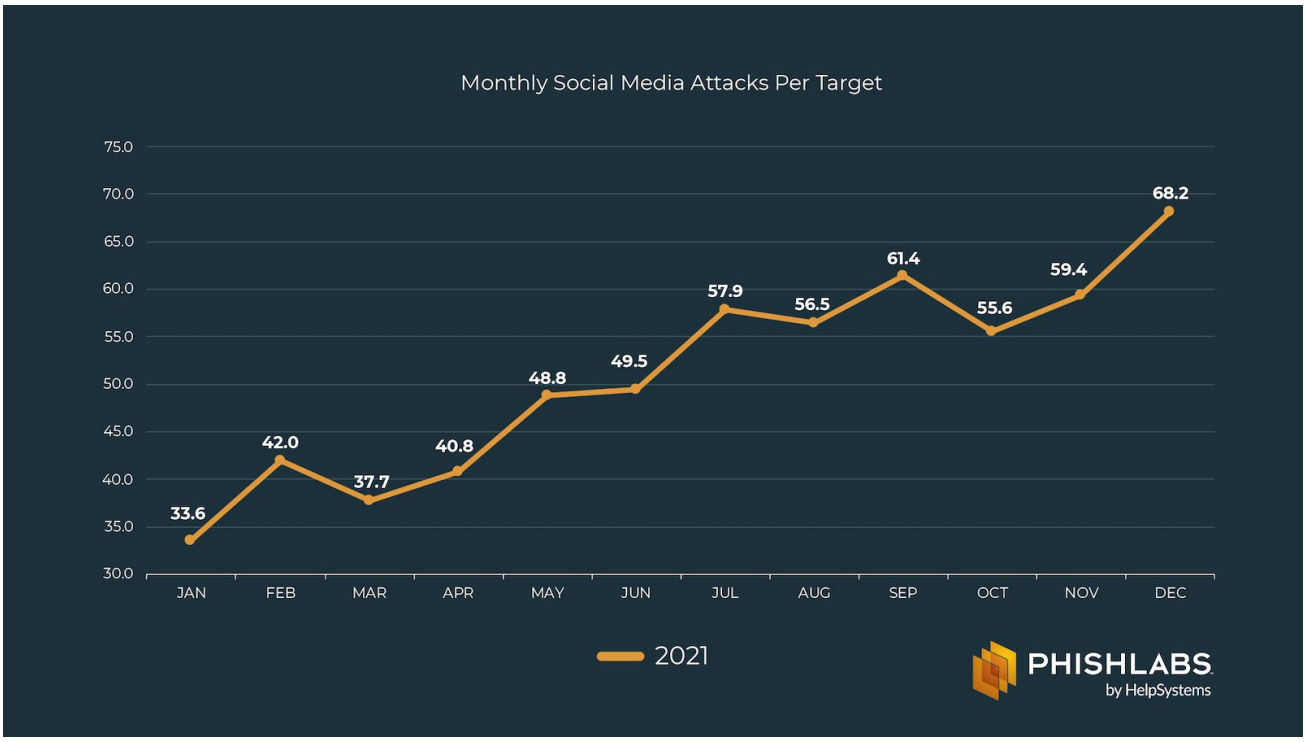
Vishing Attacks Are at an All-Time High, Report Finds

Vishing attacks have increased almost 550 percent over the last twelve months, according to Agari and PhishLabs' Quarterly Threat Trends & Intelligence Report.



Qbot Payloads Dominate Q1

Qbot payloads targeting enterprises contributed to almost three quarters of all email-based malware since the beginning of 2022.



Social Media Attacks Double in 2021 According to Latest PhishLabs Report

Social Media attacks targeting organizations increased 103% in 2021, according to PhishLabs' Threat Trends & Intelligence Report.