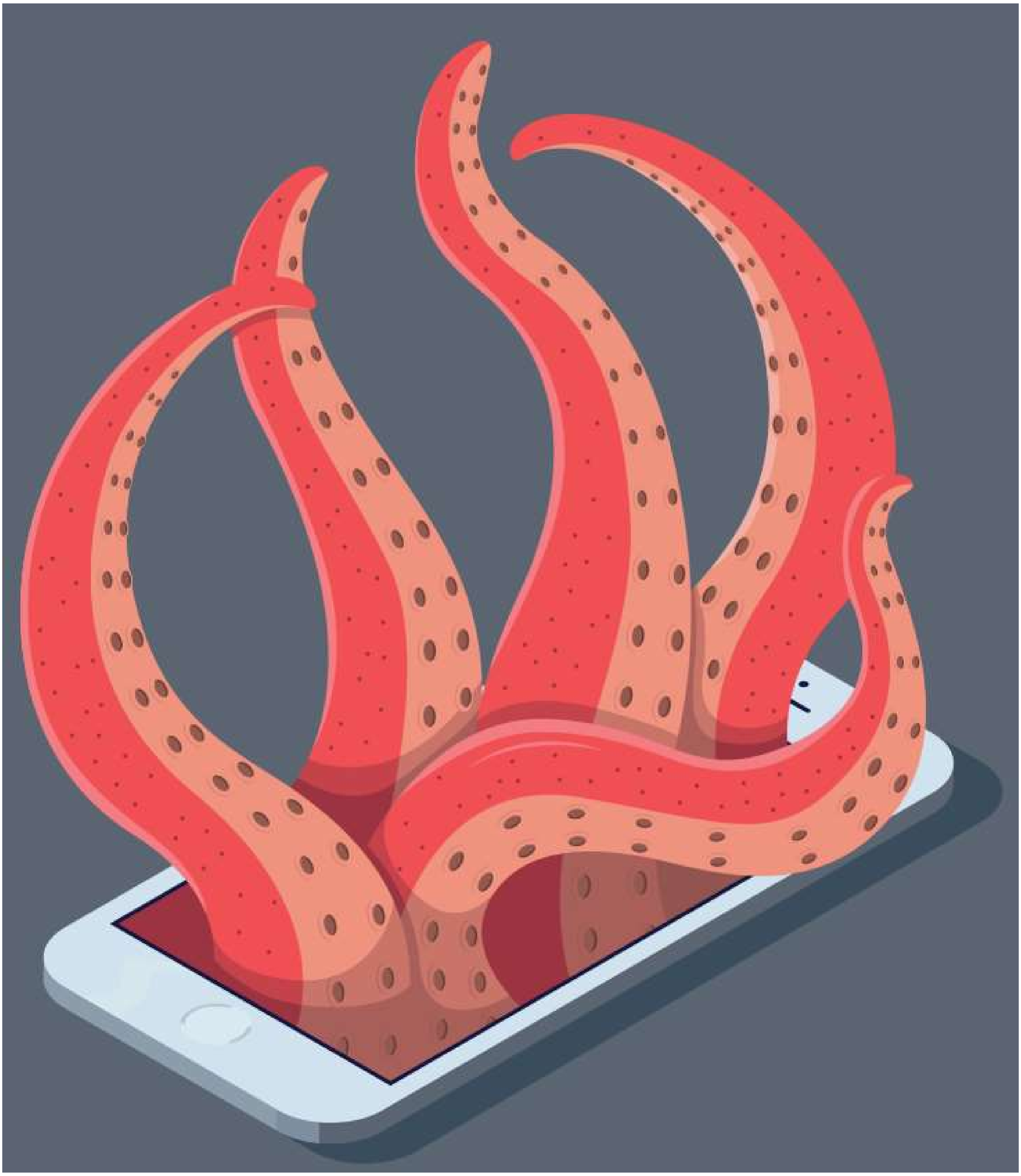
KrebsonSecurity
In-depth security news and investigation

When Low-Tech Hacks Cause High-Impact Breaches

February 26, 2023

12 Comments

Web hosting giant **GoDaddy** made headlines this month when it disclosed that a multi-year breach allowed intruders to steal company source code, siphon customer and employee login credentials, and foist malware on customer websites. Media coverage understandably focused on GoDaddy's admission that it suffered three different cyberattacks over as many years at the hands of the same hacking group. But it's worth revisiting how this group typically got in to targeted companies: By calling employees and tricking them into navigating to a phishing website.



In a filing with the **U.S. Securities and Exchange Commission** (SEC), GoDaddy said it determined that the same “sophisticated threat actor group” was responsible for three separate intrusions, including:

-March 2020: A spear-phishing attack on a GoDaddy employee compromised the hosting login credentials of approximately 28,000 GoDaddy customers, as well as login credentials for a small number employees;

-November 2021: A compromised GoDaddy password let attackers steal source code and information tied to 1.2 million customers, including website administrator passwords, sFTP credentials, and private SSL keys;

-December 2022: Hackers gained access to and installed malware on GoDaddy's cPanel hosting servers that "intermittently redirected random customer websites to malicious sites."

"Based on our investigation, we believe these incidents are part of a multi-year campaign by a sophisticated threat actor group that, among other things, installed malware on our systems and obtained pieces of code related to some services within GoDaddy," the company stated in its SEC filing.

What else do we know about the cause of these incidents? We don't know much about the source of the November 2021 incident, other than GoDaddy's statement that it involved a compromised password, and that it took about two months for the company to detect the intrusion. GoDaddy has not disclosed the source of the breach in December 2022 that led to malware on some customer websites.

But we do know the March 2020 attack was precipitated by a spear-phishing attack against a GoDaddy employee. GoDaddy described the incident at the time in general terms as a social engineering attack, but one of its customers affected by that March 2020 breach actually spoke to one of the hackers involved.

The hackers were able to change the Domain Name System (DNS) records for the transaction brokering site **escrow.com** so that it pointed to an address in Malaysia that was host to just a few other domains, including the then brand-new phishing domain **servicenow-godaddy[.]com**.

The general manager of Escrow.com found himself on the phone with one of the GoDaddy hackers, after someone who claimed they worked at GoDaddy called and said they needed him to authorize some changes to the account.

In reality, the caller had just tricked a GoDaddy employee into giving away their credentials, and he could see from the employee's account that Escrow.com required a specific security procedure to complete a domain transfer.

The general manager of Escrow.com said he suspected the call was a scam, but decided to play along for about an hour — all the while recording the call and coaxing information out of the scammer.

"This guy had access to the notes, and knew the number to call," to make changes to the account, the CEO of Escrow.com told KrebsOnSecurity. "He was literally reading off the tickets to the notes of the admin panel inside GoDaddy."

About halfway through this conversation — after being called out by the general manager as an imposter — the hacker admitted that he was not a GoDaddy employee, and that he was in fact part of a group that enjoyed repeated success with social engineering employees at targeted companies over the phone.

Absent from GoDaddy's SEC statement is another spate of attacks in November 2020, in which unknown intruders redirected email and web traffic for multiple cryptocurrency services that used GoDaddy in some capacity.

It is possible this incident was not mentioned because it was the work of yet another group of intruders. But in response to questions from KrebsOnSecurity at the time, GoDaddy said that incident also stemmed from a "limited" number of GoDaddy employees falling for a sophisticated social engineering scam.

"As threat actors become increasingly sophisticated and aggressive in their attacks, we are constantly educating employees about new tactics that might be used against them and adopting new security measures to prevent future attacks," GoDaddy said in a written statement back in 2020.

Voice phishing or "vishing" attacks typically target employees who work remotely. The phishers will usually claim that they're calling from the employer's IT department, supposedly to help troubleshoot some issue. The goal is to convince the target to enter their credentials at a website set up by the attackers that mimics the organization's corporate email or VPN portal.

Experts interviewed for an August 2020 story on a steep rise in successful voice phishing attacks said there are generally at least two people involved in each vishing scam: One who is social engineering the target over the phone, and another co-conspirator who takes any credentials entered at the phishing page — including multi-factor authentication codes shared by the victim — and quickly uses them to log in to the company's website.

The attackers are usually careful to do nothing with the phishing domain until they are ready to initiate a vishing call to a potential victim. And when the attack or call is complete, they disable the website tied to the domain.

This is key because many domain registrars will only respond to external requests to take down a phishing website if the site is live at the time of the abuse complaint. This tactic also can stymie efforts by companies that focus on identifying newly-registered phishing domains before they can be used for fraud.

GoDaddy's latest SEC filing indicates the company had nearly 7,000 employees as of December 2022. In addition, GoDaddy contracts with another 3,000 people who work full-time for the company via business process outsourcing companies based primarily in India, the Philippines and Colombia.

Many companies now require employees to supply a one-time password — such as one sent via SMS or produced by a mobile authenticator app — in addition to their username and password when logging in to company assets online. But both SMS and app-based codes can be undermined by phishing attacks that simply request this information in addition to the user's password.

One multifactor option — physical security keys — *A U2F device made by Yubikey.*
appears to be immune to these advanced scams.
The most commonly used security keys are inexpensive USB-based devices. A security key implements a form of multi-factor authentication known as Universal 2nd Factor (U2F), which allows the user to complete the login process simply by inserting the USB device and pressing a button on the device. The key works without the need for any special software drivers.

The allure of U2F devices for multi-factor authentication is that even if an employee who has enrolled a security key for authentication tries to log in at an impostor site, the company's systems simply refuse to request the security key if the user isn't on their employer's legitimate website, and the login attempt fails. Thus, the second factor cannot be phished, either over the phone or Internet.

In July 2018, Google disclosed that it had not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical security keys in place of one-time codes.

This entry was posted on Sunday 26th of February 2023 11:15 PM

A LITTLE SUNSHINE NE'ER-DO-WELL NEWS WEB FRAUD 2.0

ESCROW.COM GODADDY BREACH DECEMBER 2022 GODADDY BREACH MARCH 2020 GODADDY BREACH NOVEMBER 2020 GODADDY BREACH NOVEMBER 2021 VISHING VOICE PHISHING

12 thoughts on "When Low-Tech Hacks Cause High-Impact Breaches"

RSS

February 27, 2023

First, and why does this only show up in RSS

masterX244

-

February 27, 2023

Front page is heavily cached. it takes a bit until those expire and the content is reloaded.

The Sunshine State

February 27, 2023

My opinion on Godaddy(.)com, they are a huge register of domains for the use of spamvertised and phishing websites

Eric

-

February 28, 2023

My opinion is any tech company that used buxom half-dressed models to sell their services didn't take themselves seriously, so I didn't either.

Ted leaf

February 27, 2023

You would think large firms like godaddy, hardly short of a few dollars, having seen how effective cheap USB keys are at other places like Google, would go all out to start using the same systems themselves, keys are what, about $50 for the more sophisticated ones, half that for still adequate ones, hardly bank breaking, even cheaper in bulk orders I should think, $1 per week per employee to guarantee that at least a lot of commonly used methods for hacking systems just won't work..
Makes you wonder even more about some firms priorities and tends to re-enforce my habit of avoiding them and their clients as much as possible..

dallasmediator

February 27, 2023

Sophisticated: the hacker knows more than the idiots we hire at GoDaddy
threat: bad things that happens that affect my stock price
actor: they hurt me
group: more than one

DaBunny

February 27, 2023

Kinda agree with Ted here. It's been half a decade since Google went to U2F. Why isn't that considered to be best required best practice at this point?

Paul S

February 27, 2023

One issue / problem with U2F devices is that an alternate method to verify login credentials is employed in case of loss of the U2F device or simple inability to access the device at that moment. This can rely on SMS messages for example. It is advisable to register more than one U2F device so that loss of one can be overcome by use of the second device. It is still the case that we humans are the weak link.

AJ42

-

March 1, 2023

Apple's new Passkey technology is U2F underneath, if you have an iphone to receive an SMS, you have the same iphone to use more secure U2F. The solution is to get both a physical token and your iphone. One is used for daily auth, the other is for a backup. A well documented backup strategy needs to be communicated.

hera

March 1, 2023

This is very nice and this article is very helpful for everyone. I hope it becomes a useful website and has quality articles to educate everyone.

IPTV Smarters APK

March 1, 2023

It's been half a decade since Google went to U2F. Why isn't that considered to be best required best practice at this point?

Paul

March 3, 2023

One thing I haven’t seen mentioned in all the coverage on GoDaddy is that their Cpanel doesn’t have the option of MFA. I called them and asked why not and they said something like because it’s a shared system they can’t do it. My main host has MFA and I don’t know why they don’t. O365 through GoDaddy has MFA, Their main site has MFA but their Cpanel that gives access to just about everything doesn’t.