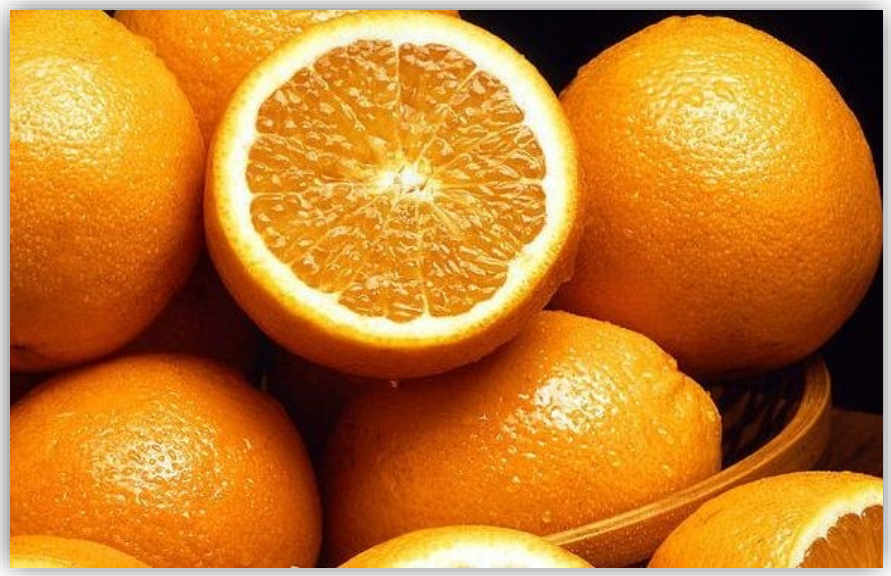
TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

May 2018

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.



Orangeworm Hacker Group Attacks Health Care Sector

A recent report from Symantec's Security Response Attack Investigation Team has zeroed-in on a hacking collective that is harassing the health-care industry. The group's name has been found to be Orangeworm and they have been responsible for hacking various health-care-related targets in the United States, Europe, and Asia. The group was previously unidentified when they first popped-up on researchers' radars in 2015, but now their methodology and identity is well-documented.

Symantec noted the following about Orangeworm's targets: "*Based on the list of known victims, Orangeworm does not select its targets randomly or conduct opportunistic hacking.*

Rather, the group appears to choose its targets carefully and deliberately, conducting a good amount of planning before launching an attack."

The main attack method for Orangeworm is installing a backdoor via the Trojan Kwampirs. Kwampirs has been discovered on software for X-Ray and MRI machines, on systems connected to networks with highly sensitive data, and anything else remotely related to powerful healthcare corporations.

Once the backdoor has been installed, and the target has been confirmed to be of interest, the first thing Kwampirs does (after decrypting and extracting the DLL payload) is "aggressively copy the backdoor across open network shares to infect other computers."

Symantec notes the following hidden file shares as common places for the backdoor to dig into the network:

- ADMIN$
- C$WINDOWS
- D$WINDOWS
- E$WINDOWS

The main purpose of all of this is an aggressive form of reconnaissance, which is thought to possibly be linked to corporate espionage. The amount of internal data recovered from these attacks can prove very useful as they encompass not only data from the company but also any business partner the company may deal with.

Symantec notes that the Orangeworm hackers aren't particularly concerned with stealth. The attacks they carry out are what we in the security field call "loud" and are prone to set off any alert mode that IT departments respond to (for example, their IDS or IPS). A big reason why such a reckless approach works is that many health-care industry leaders still run Windows XP, which is much easier to penetrate and stay on due to primitive security protections.

This last point is so crucial as cybersecurity professionals have warned against the dangers of running obsolete OS variants like XP for years. There have been constant warnings that issues would reach critical mass, and once they did with WannaCry, I thought there might be a change. Obviously, the change wasn't enough as Orangeworm is proving that XP is still widely in use in such a sensitive industry.

Health-care executives: **Update your OS or continue to be vulnerable to these attacks.**

3 Changes the NHC is Implementing for the Upcoming 2018 Hurricane Season

The 2017 Atlantic hurricane season was one for the record books, and as people prepare for what the upcoming hurricane season brings, they may notice changes that the National Hurricane Center (NHC) is making.

The Atlantic Hurricane season begins on June 1 and lasts through Nov. 30, reaching its peak around the middle of September. People that live near the the coast should be mindful of developing or ongoing tropical systems during this time and take action if one is forecast to impact their area.

This year, the National Hurricane Center (NHC) is making some changes to maps and other products to help improve communication to the public, including where a tropical system is headed and what impacts it may bring.

Here are three changes that the NHC is making for the upcoming hurricane season:

1. Adjustments to the official hurricane track maps

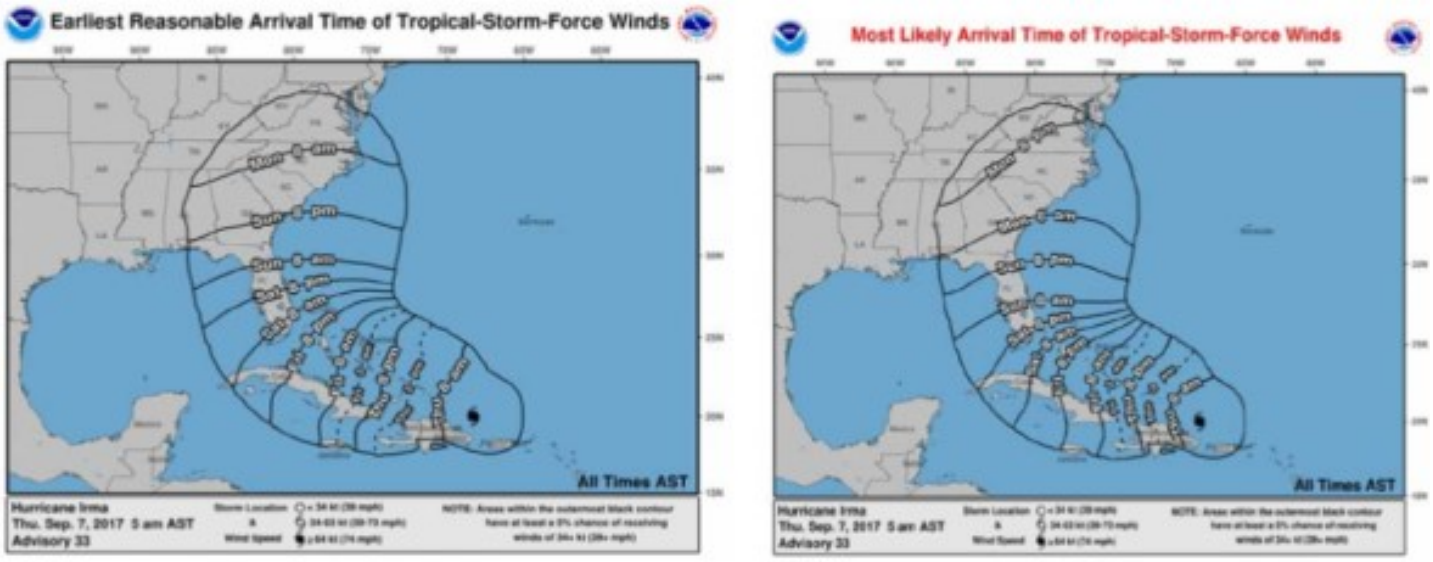
One of the biggest changes this hurricane season will be adjustments to the NHC's hurricane track map. When the NHC issues a track for a tropical system, the map includes what is known as the cone of uncertainty.

"The cone represents the probable track of the center of a tropical cyclone, and is formed by enclosing the area swept out by a set of imaginary circles placed along the forecast track," the NHC said.

For the 2018 Atlantic hurricane season, the cone will be smaller than it has been in past years. This will give the public a better idea of where the center of the storm is headed in the coming days. This cone will likely shrink more in the coming years as the accuracy of forecasts and weather models continues to improve.

2. Experimental wind maps will become official

In 2017, the NHC introduced an experimental map to help convey to the public when strong winds would arrive at a given location. These experimental maps showed the expected arrival time of tropical storm-force winds in 6- to- 12-hour increments extending out five days out.



“The arrival of sustained tropical-storm-force winds is a critical planning threshold for coastal communities, as many preparedness activities become difficult or dangerous once winds reach tropical storm force,” the NHC said.

After going through a test run in the 2017 season, the NHC has decided to make these maps fully operational for the upcoming season. The NHC will be issuing two different maps showing variations of the expected arrival times.

“One is the 'earliest reasonable time' one could expect tropical-storm-force winds within the forecast cone," AccuWeather Hurricane Expert Dan Kottlowski said. “The second is the 'most likely' time one could expect tropical-storm-force winds to reach a given location within the forecast cone.”

3. Advisories will include potential impacts farther in advance

Whenever there is an active tropical system, the NHC issues a public advisory that includes information about all aspects of the storm, such as current winds, expected storm surge and the precise location of the system's center.

In past years, these advisories only discussed the given tropical system for the next two days, limiting the amount of log-range details about the storm.

2018's Cutting Edge Network Security Solution:

Cisco Umbrella

Cloud Delivered Enterprise Security

As the industry's first Secure Internet Gateway in the cloud, Cisco Umbrella provides the first line of defense against threats on the internet.

As a secure internet gateway, Cisco Umbrella helps you tackle the challenges of mobility, SaaS, and branch transformation by offering a single platform that secures access to and use of the cloud, SaaS applications, branch offices, and endpoints.

It's your first line of defense against threats -- anytime and anywhere your users access the internet, traffic goes through Umbrella first. By delivering security from the cloud, not only do you save money, but it also provides more effective security. Here's how:

1. DNS & IP layer enforcement

Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

2. Intelligent proxy

Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection.

3. Command & control callback blocking

Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers. Stop data exfiltration and execution of ransomware encryption.

Call Tech Hero today to sign up for your free trial!

(800) 900-8324 x2

However, starting this year, these advisories will contain information that talks about hazards as far as five days in advance.

"This will better explain possible track and intensity chances or potential changes and forecast challenges," Kottlowski said.

This extra information will help to save lives and protect property by providing people with possible impacts well ahead of the storm's arrival, especially when forecasters have high confidence with a particular storm.

Client Spotlight

easterseals Florida

Easterseals Florida is the leader in providing exceptional services, education, outreach, and advocacy so that people living with autism and other disabilities can live, learn, work and play in our communities. We are honored to be Easterseals Florida's managed services provider for the past 17 year.

To donate to this amazing organization please visit: www.easterseals.com/florida/

Would you like your company highlighted here in our "Client Spotlight"?
Then give us a call today at 1-800-900-8324 x8840.

10 Things To Consider When It Comes To Disaster Recovery

Just as you would prepare your property ahead of a storm, it is vital for businesses to understand their risk profile to ensure the availability and redundancy of their IT operations before any natural disaster. A good first step is for businesses to partner with a data center provider. But how do you know you've chosen a partner who can handle any challenge? Organizations must be confident their data center provider has a solid emergency response plan in place to ensure their own operational integrity, as well as the security and availability of their most important data.

Here are ten considerations to keep in mind when choosing a disaster recovery (DR) provider:

1. Begin planning for an emergency long before it happens

You should put considerable effort into advanced planning. Make sure your data center provider uses a thorough and systematic program that combines

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

preventative maintenance, infrastructure monitoring, staff training and assessments. These initial steps lay the groundwork for minimizing and even avoiding potential downtime.

2. Focus on location

Preparedness begins with choosing a data center in the right location. When evaluating providers, be sure to ask questions such as does the provider offer the geographic diversity necessary to ensure its customers can continue operations through other facilities if their primary data center is disabled? Are data centers located outside of flood zones and away from fault lines?

3. Ensure Redundancy

To sustain an uninterrupted power supply, your provider should utilize redundant power supply (UPS) systems and generators -- each with N+1 configurations. Multiple computer room air conditioning units with N+1 configurations maintain a sufficiently regulated IT environment if one cooling system goes down.

4. Preventative maintenance

Make sure your provider is proactively protecting its critical systems to optimize performance and availability for its customers. Regular preventative maintenance and testing should be performed on key emergency systems like generators, UPSs, cooling systems, fire detection and suppression systems.

5. Look at the physical security of operations

Does your data center provider's staff monitor its network and facilities 24/7/365 to ensure the safety and security of its operations? It is important to have eyes and ears on the ground as it can be a key component in their ability to effectively mitigate damage.

6. Always have a backup plan

It's always a good idea to maintain relationships with outside vendors to ensure someone has your back in the event of a disaster. A good data center provider will have strong relationships with multiple Tier One internet providers, in case they need to quickly transition between carriers without service interruption should one carrier go down.

7. Check your data center has multiple fuel providers

Having generators won't matter if your fuel supply chain breaks down. Make sure your data center provider has at least three fuel providers -- two in-state and one out-of-state -- to service data centers during an extended outage.

8. Test you plan

Make sure your provider regularly tests its plans for emergency preparedness, response and recovery through live exercises during normal operations. There's no such thing as being too prepared.

9. Establish a 'go team'

It is important for a provider to have an established geo-diverse group of individuals who are highly trained and experienced in network and data center operations and emergency response. This team should participate in intense training to hone their preparedness for any situation and members should be cross-trained to perform multiple roles to ensure operational

redundancy in an emergency. The go team can be used to relieve local teams, allowing them to focus on keeping their homes and families safe.

10. Don't forget about backup supplies

Make sure your provider has the supplies to support your employees if they need to remain at the data center throughout the storm. Nothing says "We value our customers" like keeping a pantry stocked with food, water, bedding and other necessary provisions.

You can even take your organization one step further, by enlisting the help of a trusted vendor who can provide an added layer of support during a storm or natural disaster. Consider these added measures to support your DR planning efforts:

- **Business continuity and DR software:** Consider a solution capable of protecting, recovering and mobilizing applications on virtualized IT
- environments, including public, private and hybrid clouds.
- **A cloud data management platform:** Hybrid cloud enterprises need to
- orchestrate data in a way that is easy to manage and future-proof.
- **Additional data protection:** Whether you operate at a mid-size or
- enterprise-level-system size, you need a partner that can deliver flexible solutions that best fit your organization's needs. Find a provider that offers data protection and information management solutions that can help turn your data into a powerful strategic asset your organization can access safely and securely.

Ensuring your DR provider, a third-party vendor or your IT organization has a solid plan in place to deal with disasters -- both natural and man-made -- must be a top priority. If not, you risk not only the safety of your data and applications but of your entire business.