



PERCH



H-ISAC™

HEALTH - ISAC

QUARTERLY THREAT BRIEF

# Healthcare Heartbeat

Cybersecurity Trends  
and Threats for the  
Healthcare Sector

Q3 2020

TLP:WHITE

# Introduction

Health-ISAC and Perch Security have created a joint report covering the top cyber threat trends that the healthcare sector faces. The purpose of this report is to share some of the threats and attack trends across the healthcare industry that Perch Security, in collaboration with Health-ISAC, have observed over the last quarter.

Health-ISAC member products and services are both augmented and supported by trusted intelligence partner relationships. The Perch/Health-ISAC relationship is unique in that analysts from both Perch and Health-ISAC exchange timely relevant threat intelligence collected and secured within Health-ISAC's Threat Operations Center (TOC) in Titusville, FL. This unique relationship creates opportunities to collaborate on threats facing the healthcare sector supported with real-time sensor flow of network security data to provide critical insights to member organizations.

# Executive Summary

The third quarter of 2020 saw continued growth in cyberattacks against healthcare organizations across the globe. The remote workforce brought on by COVID-19 has created a unique set of challenges for information security providers and high-value targets for threat actors. The unfortunate resurgence of Emotet has been a continuous source of pain and initial access into organizations across the world. Further, ransomware damages and related disruptions to patient care is the number one issue facing the healthcare sector. As always, the goal of Health-ISAC is to serve our membership as effectively as possible to ensure patient care goes unaffected in continually difficult times. This Threat Report serves to provide guidance and information regarding these key threats.

## Foreword from Health-ISAC

Pharmaceutical firms continue crucial research and development to develop COVID-19 vaccines and treatments. Healthcare providers care for patients infected with the virus. The global healthcare sector proceeds with their respective missions. These global healthcare sector businesses perform their crucial missions while cyber threats like ransomware worsen.

The Perch and Health-ISAC partnership is so valuable, in my opinion, because reports like this bring quantitative and qualitative reality to life. We're not just guessing these threats exist. We know it because we see it in Perch's reporting – and we see specifically impacting Perch's healthcare clients.

I encourage healthcare firms to learn from the threats discussed here, use it to explain the sector threats to your senior leadership, hopefully get more resources and implement the recommendations detailed here.

**Errol Weiss, CSO**

## Foreword from Perch Security

“Perch Security provides threat detection and response services for thousands of organizations around the world, and as such, our primary focus is knowing what it takes to keep systems and users safe. The threats we see today are numerous and growing, but one thing that has not changed is the success of phishing. The biggest threat we have observed to our customer's networks is ransomware, with environments commonly compromised through phishing. New vulnerabilities such as ZeroLogon have also emerged, giving attackers a strong path for privilege escalation after a successful phish.”

**Taylor Green, SOC Director**

# Threat Trends in the Healthcare Sector

## Malware

Perch and Health-ISAC have identified two critical malware families that are targeting the healthcare industry with a high level of success during Q3 2020. Malware comes in many forms, but there are a few types that are consistently successful and have a large, well-funded support infrastructure behind them. For these reasons, we believe emphasizing and bolstering protections against the specific types identified is critical for healthcare organizations. These malware families are:

1. Emotet

Emotet is the term for both the malware and its operators. A resurgence of Emotet activity has been assaulting the globe with sophisticated and targeted phishing campaigns that implant Emotet malware. The primary delivery payload is a malicious Word document (.doc) attachment through a phishing email that will download more files from Emotet-controlled infrastructure. Emotet is a consistently successful initial access mechanism that leads to ransomware activities. Significant resources and guides are referenced in this report that outline the techniques, tactics, and procedures (TTPs) implemented by this malware, as well as recommendations for both preventing and remediating an infection.

2. Trickbot

Another long-running trojan and botnet, Trickbot, has become a staple for malicious actors. The Trickbot malware is modular software that can capture credentials, perform internal reconnaissance, exfiltrate data, and receive further data through Trickbot infrastructure. The successes of the operators over the years have led to one of the largest botnets in the world, with claims of over one million compromised machines. In turn, this infrastructure has become provided “as a service” to other threat actors for other campaigns, most notably for deploying Ryuk ransomware against a compromised organization. Recently, a joint effort was underway between Microsoft, FS-ISAC, major telecommunications providers, and other agencies to perform a large-scale takedown of US-based Trickbot infrastructure. This had significant disruptions to their operations, but Trickbot activity has persisted and will continue to be a serious threat.

3. Qbot

We highlighted Qbot during the previous quarter and, unfortunately, it has persisted as a major threat. Qbot is a trojan that implements obfuscation techniques and, once on a system, looks to establish persistence through scheduled tasks and registry edits to communicate externally, spread inside a network, and inevitably exfiltrate any sensitive information found. Qbot malware typically functions like a banking trojan with financial motivations but has recently moved in the direction of Emotet and Trickbot, where it serves as a dropper for ransomware. Financially motivated threat actors looking to maximize profitability are altering their malware to leverage the

Ransomware-as-a-Service (RaaS) trends discussed further below.

## **Ransomware**

Organizations within the healthcare sector are especially vulnerable to ransomware. Patient safety may become compromised, from risks of private health information leakage or critical infrastructure disruption. This quarter, we are focusing on the observed trends in ransomware activity, what the threat actors in this space are doing, recommendations to combat them, and some government guidance for ransom payments.

The Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Ransomware Guide on September 30th that should be essential reading for all IT professionals. Some of the highlights include references to specific ISAC resources, a “Best Practices” checklist, a breakdown of how ransomware attacks often occur, and response resources. We strongly encourage Health-ISAC members to review this guide and incorporate its recommendations into your security posture.

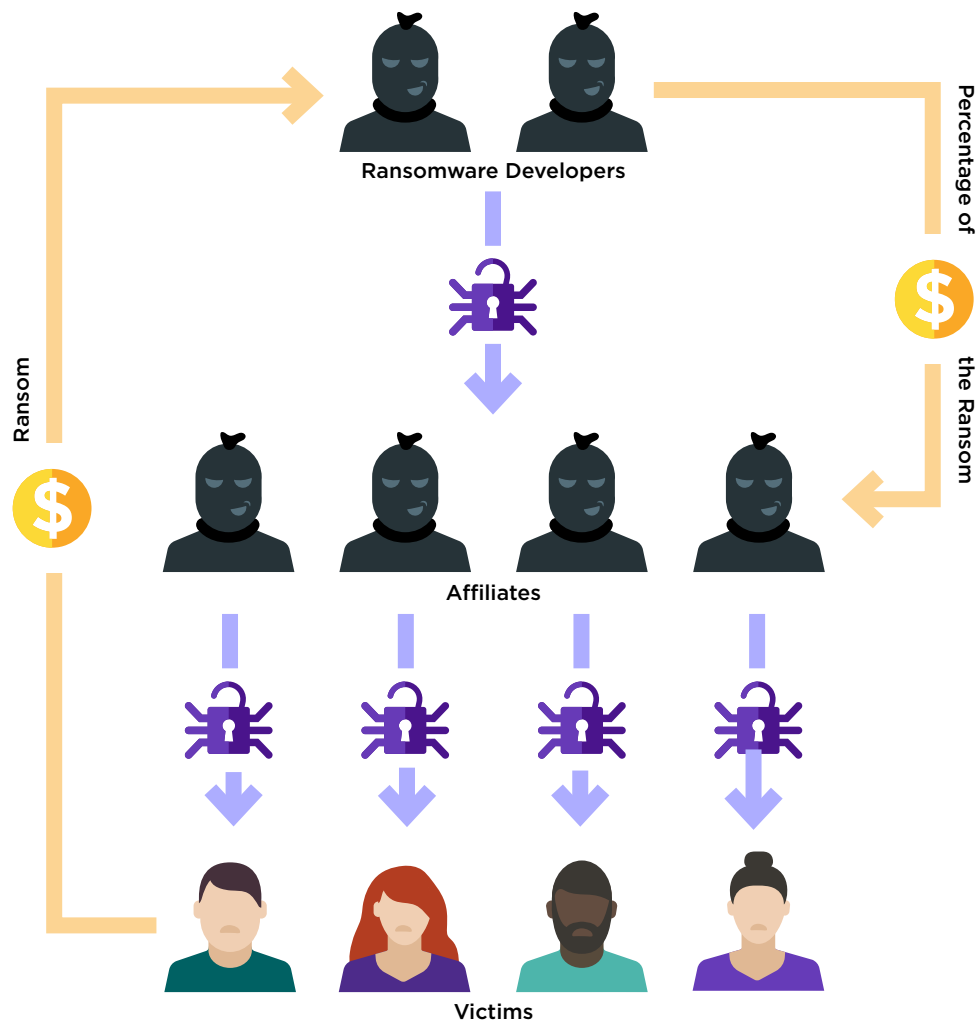
<https://us-cert.cisa.gov/Ransomware>

The ransomware threat landscape has continued to evolve. In Q3 2020, we saw the development of “ransomware gangs,” with multiple groups working together on distributed elements of the ecosystem from development to initial access to payment management.

### **Here are the key trends from the third quarter of 2020:**

#### **1. Ransomware-as-a-Service**

The proliferation of Ransomware-as-a-Service (RaaS) continues to dominate the threat landscape. The distributed nature of the most successful threat actors over the last several months speaks to the efficacy of the RaaS model. The criminal underground has opened the floodgates by allowing anyone with the savvy and will to sell initial access to ransomware operators for a fee. This has led to a surge in reconnaissance and attempted sale of access into organizations of all kinds. Hospitals, medical companies, and their records continue to be a primary target for these types of RaaS activities, as the value is comparatively high for a successful attack.



## 2. Ransom, Extortion after Data Exfiltration, and now Denial of Service

In the inaugural Healthcare Heartbeat report, we identified the compounding of damage and profitability for ransomware operators to both lock systems in demand for payments and charge for the exfiltrated data to not be sold. Now, we are seeing a third mechanism for profit where threat actors are leveraging a Denial of Service attack against critical systems to demand payment as well. This concept of “Triple Dipping” has created greater difficulties in the restoration process after compromise and should be included in planning efforts.

## 3. U.S. Treasury Notice on Ransom Payments

On October 1st, the United States Department of the Treasury, through the Office of Foreign Assets Control (OFAC), posted an advisory titled, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.” Federal regulatory powers against financial engagements with sanctioned foreign powers can now be applied to ransom payments in the name of national security. This will likely have significant impacts on the

ransomware landscape as ransom payments are now considered potential sanctions violations by the Treasury. We encourage members to review information around the OFAC advisory.

#### 4. Public Relations

In a strange spectacle, threat actors operating some of the largest ransomware gangs have been attempting to improve their “brands” through public relations activities. Previously, we saw several groups state they would not be targeting healthcare organizations throughout the coronavirus pandemic, but that has obviously not applied to all actors. We are now seeing several threat actors claim that portions of their ransom payments are being “donated to charity.”

## Recommendations

1. Ensure that you are maximizing the benefits of your Health-ISAC membership. There are several ways to ingest threat intelligence into your environment automatically:
  - Anomali
  - Perch
  - TruStar
  - STIX/TAXII
  - Health-ISAC Automated Threat Intelligence Feeds
2. Give back to the community! Keeping other healthcare organizations safe is a worthwhile effort, and the membership is only as strong as those of us who work together.
3. Reach out to the Health-ISAC Threat Operations Center for information and educational opportunities around leveraging and implementing Health-ISAC Automated Threat Intelligence.
4. **Health-ISAC Situational Awareness Platform** - Ensure that you are staying up to date on healthcare sector news and information through the Daily Cyber Headlines, event-driven Threat Bulletins, monthly Threat Briefs, and more that are developed and distributed through Health-ISAC's Cyware Situational Awareness Platform (CSAP).

Health-ISAC members should be sure to check out the detailed TLP:**AMBER** version of this quarterly report, available through the member-only mailing lists and the Cyware Threat Intelligence Portal. Contact Health-ISAC membership services if you need assistance locating the report ([membership@h-isac.org](mailto:membership@h-isac.org)).